

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 VS.) No. 4:16-CR-258 (CEJ/NAB)
)
 ALDEN DICKERMAN,)
)
 Defendant.)
 _____)

EVIDENTIARY HEARING
BEFORE THE HONORABLE NANNETTE A. BAKER
APRIL 19, 2017
ST. LOUIS, MISSOURI

FOR THE PLAINTIFF:

COLLEEN C. LONG
ROBERT LIVERGOOD
OFFICE OF U.S. ATTORNEY
111 South Tenth Street, Suite 2000
St. Louis, MO 63102
(314) 539-2200

FOR THE DEFENDANT:

ADAM D. FEIN
MARC JOHNSON
ROSENBLUM SCHWARTZ, PC
120 S. Central Avenue, Suite 130
St. Louis, MO 63105
(314) 862-4332

Proceedings recorded by mechanical stenography;
transcript produced by computer.

DEBORAH A. KRIEGSHAUSER, FAPR, RMR, CRR
Federal Official Court Reporter
111 South Tenth Street, Third Floor
St. Louis, MO 63102
(314) 244-7449

I N D E X

APRIL 19, 2017

Plaintiff's

<u>Witnesses:</u>	<u>Direct</u>	<u>Cross</u>	<u>Redirect</u>	<u>Recross</u>
-------------------	---------------	--------------	-----------------	----------------

S.I. WAYNE BECKER	5	43	98	105
-------------------	---	----	----	-----

DET. MICHAEL SLAUGHTER	107	129	140	143
------------------------	-----	-----	-----	-----

DR. BRIAN LEVINE	145	174	193	---
------------------	-----	-----	-----	-----

Defendant's

<u>Witnesses:</u>	<u>Direct</u>	<u>Cross</u>	<u>Redirect</u>	<u>Recross</u>
-------------------	---------------	--------------	-----------------	----------------

HON. JOHN BORBONUS	195	219	228, 230	230
--------------------	-----	-----	----------	-----

1 (PROCEEDINGS BEGAN AT 9:30 AM.)

2 THE CLERK: All rise. This Court is back in session.
3 You may be seated.

4 THE COURT: Good morning. We are on the record now
5 in the case of *United States of America versus*
6 *Alden Dickerman*. Mr. Dickerman has filed Motions to Suppress
7 Evidence and Statements, and he's also filed a motion for a
8 *Franks* hearing, and so that's the purpose of today's hearing.

9 What I would like to do is start by having counsel
10 announce your presence for the record.

11 MS. LANG: Colleen Lang for the Government.

12 MR. LIVERGOOD: Robert Livergood on behalf of the
13 Government.

14 MR. FEIN: Adam Fein on behalf of the Defendant, and
15 Mr. Dickerman is present in the courtroom, Your Honor.

16 THE COURT: Thank you.

17 We can go ahead and get started with the proceedings.
18 The Government -- I have had an opportunity, of course, to
19 review the briefing in this case. It is -- It appears that we
20 have some novel issues, I would say.

21 So I understand -- The Government, how many witnesses
22 will you have today?

23 MS. LANG: I have three witnesses, Your Honor.

24 THE COURT: And for the Defendant?

25 MR. FEIN: Two, perhaps three; most likely two.

1 THE COURT: Okay. All right. At this time the
2 Government may call their first witness.

3 MS. LANG: Thank you, Your Honor. The Government
4 calls Investigator Wayne Becker to the stand.

5 THE COURT: Yes.

6 MR. FEIN: Your Honor, I don't know if there's any --
7 if there are Government witnesses present in the court right
8 now. If not, I'd at least ask the Court to invoke the rule
9 for anyone who might otherwise ---

10 MS. LANG: Detective Slaughter is here. He's out in
11 the hallway. He's my next witness. Dr. Levine will be my
12 expert witness. He is in the courtroom. It was my
13 understanding that Adam and I had an agreement that our
14 experts could sit through the proceedings.

15 MR. FEIN: That is true. That is acceptable.

16 THE COURT: Okay. So -- All right. So you all have
17 an agreement the experts will both be in the courtroom but the
18 Detective will be excluded.

19 MS. LANG: Yes.

20 THE COURT: Okay; all right.

21 MS. LANG: Thank you, Your Honor.

22 MR. FEIN: Are there any witnesses here?

23 MS. LANG: No.

24 MR. FEIN: Thank you.

25 (The Witness, SPECIAL INVESTIGATOR WAYNE BECKER,

1 Is Sworn.)

2 THE COURT: You may proceed, Ms. Lang.

3 MS. LANG: Thank you, Your Honor.

4 DIRECT EXAMINATION

5 QUESTIONS BY MS. LANG:

6 Q Please state your name.

7 A Wayne Becker.

8 Q And what's your current occupation?

9 A I'm an investigator with the Dent County Sheriff's
10 Department detached to the Missouri Internet Crimes Against
11 Children's Task Force.

12 Q And how long have you been in that position?

13 A Since 2008.

14 Q And before you were with the Dent County Sheriff's
15 Department, what was your occupation?

16 A I was in the IT industry, private sector, for 28 years;
17 various positions.

18 Q And I'm going to go ahead and move -- Well, just -- a
19 little -- What's some of the training and experience you have
20 with peer-to-peer networks as a member of the Missouri ICAC
21 Team?

22 A I've had training in a number of networks; *Aries*,
23 *Gnutella*, *BitTorrent*, and all of those at one time or another
24 I've worked cases on, and that training is provided by the
25 ICAC organization.

1 Q Do you have any training and experience with the
2 peer-to-peer program known as "*Freenet*"?

3 A Yes, I do.

4 Q And approximately what year did you begin to investigate
5 cases or look at the peer-to-peer program known as "*Freenet*"?

6 A I began looking at *Freenet* in 2011 originally.

7 Q And basically what is "*Freenet*"?

8 A *Freenet* is a peer-to-peer overlay network that uses the
9 Internet for communicating between computers running that same
10 *Freenet* software. That's why it's called "peer-to-peer"
11 because there's no central server. In those -- It has the
12 ability to exchange messages; have messaging systems --
13 there's one commonly used called "*Frost*" -- and the ability to
14 download or exchange files of various types.

15 Q And what types of files can you exchange on *Freenet*?

16 A You can exchange video files, image files, documents;
17 pretty much any -- any type of file.

18 Q And you said back in 2011 you began to kind of
19 investigate *Freenet*. What was sort of the first step into
20 figuring out what was going on on this peer-to-peer program?

21 A Well, it became -- It's very clear using the interface to
22 *Freenet* that's part of the software that IP addresses or the
23 -- of the various users are not hidden. So it doesn't attempt
24 to mask or hide who's using *Freenet*. So we could see clearly
25 who was using *Freenet*. We could also see that there was a lot

1 of child pornography activities, both files and free sites,
2 which are websites, stored in *Freenet* where child pornography
3 was available. So we began initially by -- by geolocating
4 those IP addresses, and we did some "knock and talks" to see
5 what people were doing on *Freenet*.

6 Q And did you -- How did you -- Do you know what files on
7 *Freenet* were child pornography files?

8 A We began collecting -- *Freenet* uses a key that leads you
9 to be able to rebuild the files. The file is stored in
10 pieces. It's not in any one place. It's very dissimilar to
11 other peer-to-peer networks in that you don't -- you don't
12 download the file from another user. You download it from
13 multiple users that have pieces of it, and they don't know
14 they have pieces of that file.

15 So when you insert or upload a file into *Freenet*, it
16 gets broken into these pieces in a manner that can be
17 retrieved. And then it creates a top level block that has
18 that Table of Contents for that file, called a "manifest," and
19 there's a key to that manifest, and that's what's shared to be
20 able to retrieve the file.

21 So we began collecting those keys to the manifest,
22 downloading the files and validating that they were, in fact,
23 child pornography files.

24 Q So if you're a user on *Freenet* and have it installed on
25 your computer, how would you, once you're on *Freenet*, go about

1 trying to find a file of child pornography?

2 A Well, you have to find a source for that key. There's no
3 search mechanism similar to other file-sharing systems, so you
4 can't search for -- for key words that we're familiar with.
5 So you would either find a free site that was on topic for the
6 material you're looking for or maybe a message board in the
7 message system, like *Frost*, that -- where people would
8 exchange keys to child pornography files.

9 Q And once you find a key and you're able to request it,
10 how does the system -- You said the files -- The keys are
11 broken up into little pieces and stored on all the different
12 users' computers. How does -- How does this system go about
13 reconstructing that file to get it back to the person who's
14 requested it?

15 A Well, the key to the file is a SHA256 hash of that -- of
16 that little block of the file, and all those are contained
17 within that high-level manifest block. So the first thing
18 *Freenet* would do is retrieve that manifest block which gives
19 them the Table of Contents. That gives them all the keys that
20 he needs to rebuild the file. Then he'll begin requesting
21 those blocks of his peers.

22 The peers would be the computers he's directly
23 connected to, and that will vary how many he's connected to.
24 It could be as few as 10; could be as much as 140. And -- And
25 he'll be -- he'll request, using a routing algorithm, those

1 blocks around those peers. And as he gets enough of them
2 back, he can rebuild the file.

3 Q And you said you've been doing investigations into child
4 pornography offenses on *Freenet* since approximately 2011. So
5 it's now 2017. So approximately six years you've been working
6 on this?

7 A Correct.

8 Q And how many *Freenet* investigations have you been
9 involved in?

10 A Personally, maybe 40 or 50.

11 Q And out of those 40 or 50, do you know how many --
12 once -- if the defendant's computer was discovered, they're
13 the target computer, how many turned up child pornography?

14 A We found evidence of child pornography on all of them.

15 Q And you're from -- You work with the Dent County
16 Sheriff's Office which is approximately two hours away. Did
17 the Government pay for your travel expenses for this hearing?

18 A Yes, they did.

19 MS. LANG: Your Honor, I'm now going to approach with
20 Government's Exhibits 1 through 20, and they are going to be
21 on a -- on the screen. So I have the screenshots of them, and
22 I will hand that to the officer to first admit. And I also
23 have a copy for the Defendant.

24 Your Honor, may I approach?

25 THE COURT: Yes, you may.

1 Q (By Ms. Lang) And, Investigator Becker, I've just handed
2 you what's already been marked as Government's Exhibits 1
3 through 20. Can you take a look at those? Take a look at
4 those and tell me what the first 1 through 19 are.

5 A The first -- The first 13 exhibits are what you would see
6 if you installed what a -- what an end user would do to
7 acquire *Freenet* and install it. And they're screens of the
8 various -- install process.

9 Q And so does 1 through 13 appear to be a fair and accurate
10 depiction of what the *Freenet* site looks like during the
11 install and download process?

12 A Yes, it does.

13 Q Thank you.

14 MS. LANG: And at this time I'll move to admit 1
15 through 13.

16 THE COURT: Is there any objection?

17 MR. FEIN: No, there is not.

18 THE COURT: Exhibits 1 through 13 will be admitted
19 into evidence.

20 Q (By Ms. Lang) And can you take a look at 14 through 19,
21 Investigator Becker?

22 A 14 through 19 would be an example of finding a free site
23 that contains keys to child pornography-type files and then
24 what a typical -- it looks like what a typical free site with
25 child pornography on it looks like and how you would find a

1 key to download it.

2 Q And so 14 through 19, is that a fair and accurate
3 representation of a free site that you've seen on the *Freenet*
4 network?

5 A Yes, it is.

6 MS. LANG: At this time I'd like to move to admit 14
7 through 19 for the purposes of this hearing.

8 MR. FEIN: No objection.

9 THE COURT: Exhibits 14 through 19 will be admitted
10 for purposes of this hearing.

11 Q (By Ms. Lang) And then lastly, what's marked as Exhibit
12 20, what is that just generally, Investigator Becker?

13 A It looks like a summary of the forensic findings in this
14 case.

15 MS. LANG: And at this point I'd -- For just the
16 purposes of this hearing, Exhibit 20 which is a summary slide
17 I'd like to admit.

18 THE COURT: All right. Any objection?

19 MR. FEIN: No, Your Honor.

20 THE COURT: Exhibit 20 will be admitted into
21 evidence.

22 Q (By Ms. Lang) So going to Exhibit 1, if you look at your
23 -- the screen, Investigator Becker, what is that?

24 A This is the free site project's main website, current
25 main website. For example, if you were to Google "*Freenet*," I

1 think about the first entry you would find would take you to
2 this place.

3 Q And so if you want -- This is the first page you'd see if
4 you went to *Freenet* to install it onto your computer, correct?

5 A That's correct.

6 Q And is there any price for downloading *Freenet*? Does it
7 cost anything?

8 A No. It's -- It's open source software and it's free.

9 Q And Exhibit 2, Investigator Becker, could you look at
10 that and let us know: What is Exhibit 2 showing us?

11 A Exhibit 2 would be the page you got if you selected
12 "Download" from the first page. You'd get to the download
13 page, and there's a button there. This one's specific for
14 Windows which is the majority of what we run across. You
15 would download the install file by pressing the "Download
16 Windows" button; "Download For Windows" button.

17 Q And Exhibit 3 is now on the screen. What does that show
18 us?

19 A If you downloaded it and executed the -- the install
20 file, that's the first box that would pop up to ask you what
21 language you wanted to install.

22 Q And Exhibit 4 is now on the screen. What does that show
23 on the -- well, during the *Freenet* download process?

24 A That is the -- That is the default installation folder
25 that *Freenet* will be installed into. One item noted, it

1 installs in a folder called "App Data" under Windows which is
2 a hidden folder.

3 Q And Exhibit 5, what is that?

4 A That's just asking if you want to create a "Start Menu"
5 folder for Windows called "*Freenet*."

6 Q And then Exhibit 6 is a duplicate of Exhibit 5, so we'll
7 move passed that one.

8 But Exhibit 7, what does that screen show us?

9 A That's just a summary of the install options you've
10 selected. And if you haven't selected them, it gives you
11 these defaults.

12 Q So the destination location of where the program's going
13 to be it looks like.

14 A Yes.

15 Q And then Exhibit 8?

16 A That's the complete -- After you hit the "Install"
17 button, that just tells you it's complete. If you hit
18 "Finish" and leave that checked, it'll start bringing it up.

19 Q So it's a pretty simple first five or six steps to
20 download the program.

21 A Correct.

22 Q And now Exhibit 9 on your screen, what does that screen
23 show us?

24 A Well, that's -- that's the first screen that pops up in
25 the set-up of *Freenet* the first time you run it.

1 Q And the first box, it looks like there's three -- three
2 boxes you can do. In the parentheses, it says "Low Security",
3 "High Security" or "Custom." Can you just briefly explain
4 what choosing those options are?

5 A The first two, the one of them will give you what's
6 called "Open Net" within Freenet where you connect to
7 strangers. Your peers are strangers, people that you select
8 somewhat randomly.

9 The second one is for what's called "Dark Net" which
10 -- where you only connect to friends; where it's somebody you
11 already know about that's running *Freenet* and you exchange
12 some node ID information. When I say the word "node," that's
13 just the computer running *Freenet*.

14 And the third one, I guess, is if you create some
15 hybrid or select your own security options.

16 Q And *Freenet* is a -- is an open source program, correct?

17 A That's correct.

18 Q And what does "open source" mean?

19 A It means a source code that creates the operation of the
20 program is available, so you can change the program to do
21 whatever you would like.

22 Q Okay. And then Exhibit 9-A, this was just a close-up of
23 that first box in Exhibit 9. And what is -- What's the
24 *Freenet* trying to tell us here in Exhibit 9-A?

25 A Well, it's telling you if you choose "Low Security" or

1 "Open Net," and that's the environment we're working in, if
2 you -- it's saying if you live in a relatively free country
3 where running *Freenet* is legal, you can choose this option,
4 but it's -- I mean it's safer than other peer-to-peer
5 software, but an attacker with moderate resources may be able
6 to trace your activity on *Freenet* back to you. So it's
7 warning you that -- that if you're using *Freenet*, your
8 activity can be traced in Open Net. And they -- they suggest
9 here that -- that you may want to improve security by using
10 "Dark Net" and only be connected to friends; people you know.

11 Q And law enforcement, what your -- the investigations that
12 you've done on *Freenet* only concern Open Net, correct?

13 A That's correct.

14 Q And Exhibit 10?

15 A 10's part of the install. It advises you to make sure
16 you're using incognito mode on your browser which doesn't save
17 any history.

18 Q And Exhibit 11, what does that show?

19 A Everybody running *Freenet* provides some disk storage,
20 called "data store," to it. That's where these blocks, when
21 they're scattered and stored in the network, land. You don't
22 know -- Nobody has a whole file in their data store, and you
23 really don't know what's in your data store, but that's --
24 this is where you set the size of your -- size of the data
25 store you're donating to the -- to the *Freenet* network.

1 Q So as a part of being on *Freenet*, you have to give a
2 portion of your data store to the network for storage
3 purposes.

4 A That's correct.

5 Q And Exhibit -- Exhibit 12?

6 A *Freenet* -- *Freenet* asks you how much bandwidth, how much
7 of your -- your Internet access you want to give to the use of
8 *Freenet* so it doesn't take all of your Internet capacity.
9 It'll -- It'll make an attempt to determine how much you might
10 have. And based on what you select there will determine how
11 many peers you'll connect to.

12 Q And Exhibit 13.

13 A And that's the startup screen. That's -- When you're
14 done, this is the basic browse screen that you get in front of
15 you.

16 Q So if you are on *Freenet* and you want to find a file and
17 you're on this screen, what do you do?

18 A Well, if you don't already know where to go to look for
19 it, you might collect -- select one of the index sites up at
20 the top. That would give you a number of -- An "index site"
21 is a free site that contains just a list of other free sites
22 you can go to.

23 Q So if you click on one -- Moving to Exhibit 14, if you
24 click on one of the indexes, ---

25 A This would be the -- The free site's -- The website's

1 stored in *Freenet*, called "free signs," are stored just like
2 any other file. So it has to retrieve the manifest for that
3 free site, and then it's retrieving -- What you're seeing here
4 is it's in the process of retrieving all the blocks it needs
5 in order to reconstruct the free site.

6 Q So at the top where it says, "*Freenet* is downloading the
7 page you requested," and then the file name, in this case it
8 was "Index 711," and at this point the program is downloading
9 that index for you so you can look at it, correct?

10 A Correct.

11 Q And then here, what is Exhibit 15?

12 A It would be an example of an index, one of the *Freenet*
13 indexes, and it's a list of free sites that you can collect --
14 click on. And you can see some of them are, obviously, you
15 know -- "Little Angels Lead to Heaven's" there. They're
16 clearly indicating that they're photos of nude minors.

17 Q And when you click on one of these, for example, the top
18 one, if you would click on "Dream Team Index," is that, again,
19 going to go out and look for the manifest key and rebuild
20 that?

21 A Exactly; rebuild that free site.

22 Q All right. And then going to Exhibit 16.

23 A That's an example of a -- of a fairly common format we
24 find for child pornography free sites where they're made up of
25 thumbnails. And then towards the bottom of the thing, it will

1 have a list of the keys associated with those.

2 Q So on Exhibit 17, on the bottom there, what are those
3 under the pictures?

4 A Those are the keys. Those are actually the key that you
5 need to download the file, and it contains the SHA256 hash of
6 that manifest key, an encryption key to encrypt it, and then,
7 of course, the file that you download.

8 Q So if you want a series of pictures that's -- that's
9 advertised above, you go to the corresponding key that's
10 listed there, and then you have to copy and paste that whole
11 key?

12 A Correct.

13 Q And then where do you copy and paste that key into?

14 A There's a number of places. Most commonly, you just go
15 to the "File Sharing" tab on *Freenet* and paste it into the
16 block, the bulk download box, and away you go.

17 Q And looking -- I'm now at Exhibit 18 on the screen. Is
18 that the box that you --

19 A Yes.

20 Q -- that you pasted it into?

21 A Yes. That's the download box for bulk downloads.
22 There's a number of ways you could download. You could use a
23 different -- different program or you could just do it under
24 the URL, but this is most -- probably the most common.

25 Q And when you -- when you go and paste it and it starts

1 with that -- that "CHK," when you paste that into the box and
2 you hit, you know, the "Download" button there on the screen,
3 what is the program actually doing at that point when you're
4 requesting that particular file?

5 In this case it's called "Lolita's Heaven - Abigail."

6 A What it will do is it will take the -- the media from
7 right after the "@" sign to that comma is the SHA256 hash of
8 that manifest block. That's the key to it. It'll -- It'll
9 send that to what it thinks, based on its routing number, the
10 most likely peer it's connected to that it could find there,
11 and it will begin asking for that block. And then when it
12 gets that block back, now it will have its Table of Contents,
13 all the other blocks it needs to rebuild the file, and it will
14 begin requesting those blocks.

15 Q And, for example, I was going to Exhibit 19. What's this
16 showing us?

17 A That's the start -- Somebody has started to download that
18 file.

19 Q Okay. So the user would see this, that the key that
20 they've downloaded ends with the -- in that green box the
21 "Lolita Heaven - Abigail," and then that's the progress of
22 what -- of how the download's going.

23 A That's correct.

24 Q And at this point the program is -- The request is being
25 sent out for each of the blocks on everyone's -- on the

1 different data stores on the nodes on *Freenet*, correct?

2 A At this point it hasn't found the manifest yet.

3 Q Oh.

4 A So it's still looking for that first key --

5 Q Okay.

6 A -- because it doesn't know how -- Once it gets to that,
7 now it knows how big the file is, how many blocks it has to
8 request. You know, they can track its progress after this.
9 When this image was created, it hadn't found that yet, and
10 that's why it's still zero.

11 Q Okay. And so just getting into a little bit more detail
12 about how requests actually happen on *Freenet*, if, for
13 example, you had a file that was made up of a thousand blocks,
14 what -- how many -- Well, let me rephrase that.

15 How are the -- How are the requests being sent out?

16 A Well, you have a number of peers you're connected to.
17 Ten's the minimum, and that's an easy number to do math with.
18 So if you had a thousand-block file, you need to find a
19 thousand blocks to reconstitute the file. You'll request
20 those somewhat randomly around those ten peers. So each one
21 of those peers over a course of time will get approximately a
22 hundred blocks. Some of them might get 90; some of them might
23 get 110, but somewhere around that 100 mark is what each one
24 of those ten peers is likely to get.

25 And then if that peer that got that request doesn't

1 have the block to send back, it will turn around and ask one
2 of its peers. So if you think of it in minimum terms where
3 that -- that guy also only has ten peers, well, he's going to
4 do the same thing. He's going to take that 100 blocks he
5 received and roughly spread them around that -- his ten peers.
6 Some may get 9; some may get 11; some may get 12. It will be
7 roughly around that 10-block mark. And he'll continue to do
8 that until he finds the block he's looking for.

9 And they use a facility called "Hops To Live." It
10 starts at "18" by default, and that's how many hops it will
11 take down those paths until it gives up, it can't find it, and
12 then it'll come back with a negative response that it can't
13 find the block down that peer's path.

14 Q And the -- the "HTL" or the "Hops To Live," that prevents
15 the request from basically going on forever?

16 A Correct.

17 Q Now what happened -- How do you insert -- You briefly
18 talked about this earlier, but how do you insert a file into
19 *Freenet*?

20 A A *Freenet* file sharing provides a facility to do that, so
21 I could upload a file off my computer into *Freenet*. It will
22 take it and break it into those 32 KB, those small pieces or
23 blocks, and then he will insert them the same -- kind of the
24 same way. He'll pass them to his peers based on the routing
25 algorithm and the SHA values of those blocks. And they'll

1 get -- they'll get stored where -- where the location of the
2 block in that algorithm is closest, is more retrievable. And
3 that takes some time. It will pass -- break that up and pass
4 all those blocks out. At the end of that process he'll have
5 generated a whole list of all those blocks. He will then put
6 that into a manifest key, insert the manifest key, and provide
7 that back to whoever inserted it so that the inserter will
8 then get back this long manifest key.

9 Q So if you insert, for example, like a picture of your dog
10 into *Freenet*, after it breaks it up to store the picture in
11 blocks, it'll -- the *Freenet* will send you back a manifest key
12 so you can go back to find that picture later.

13 A That's -- You need that to retrieve it, yes.

14 Q And if for some reason you don't save the manifest key,
15 would you ever be able to find that picture again?

16 A You would not.

17 Q And if no one ever requests that manifest key from
18 *Freenet*, what happens to the file?

19 A Well, *Freenet* has a finite amount of storage, and so it
20 will begin dropping blocks for files that -- or blocks that
21 never get requested. So if nobody requests the file for a
22 long enough period of time, it will get pushed out for newer
23 material that's being inserted, and then the file will
24 possibly not be able to be re -- rebuilt. It might be missing
25 blocks for the file.

1 Q So popular files on the *Freenet* system that are being
2 requested more often stay on the system.

3 A Absolutely, yes.

4 Q And are popular files that are being requested often on
5 the system, are those easier or faster to find?

6 A Yes, they can be because they're -- they're -- they don't
7 have to go maybe as many hops because they're -- they're
8 stored in more locations. And if you request a file, it will
9 cache it along the way as it -- as it brings it back. It will
10 store it temporarily. And so if it gets requested a lot, it
11 will be in those temporary stores and be retrieved very
12 quickly.

13 Q Now I'm going to move on to how offenders -- child
14 pornography offenders are located by law enforcement on
15 *Freenet*. And so you've been working on this for several
16 years. How do you go about finding a child pornography
17 offender on *Freenet*?

18 A Well, we built -- Since 2011 we began collecting keys.
19 We built a database of the -- of the keys to all those blocks
20 that make up known child pornography files for manifest keys
21 that we've located either on a free site associated with child
22 pornography or in a message board, on-topic message board.
23 And that databasing, we can match up that key and determine if
24 a request is for what we believe to be a file of interest,
25 possible child pornography.

1 Q So you have a database of known files of child
2 pornography that you can then compare to requests for these
3 same keys and SHA hash values.

4 A Correct. We then have law enforcement versions of
5 *Freenet* that -- that log the request that is sent to us. So
6 if somebody sends us a request for a block, we can log that.
7 And then later on we can process those log records by the file
8 they belong to and look for runs, streams of data related to a
9 specific file and to a specific IP address that requested it.
10 And the only IP address we can see are those that are directly
11 connected to us. So if we had ten peers, we could only
12 actually see the actual IP address of those ten. So you need
13 multiple nodes like that collecting data to start building
14 enough to be able to make cases.

15 Q And so do you monitor a law enforcement node on *Freenet*?

16 A Myself?

17 Q Yes.

18 A Yes. I have a few of them.

19 Q And just -- I don't know if we explained. What are --
20 What are "nodes" on *Freenet*?

21 A It's a computer running the *Freenet* software.

22 Q And so your peers, the law enforcement peer on *Freenet*,
23 those probably change frequently?

24 A The peers that my node is connected to?

25 Q Yes.

1 A Yeah, they'll change as people come and go off the
2 network, certainly.

3 Q And you said your -- the node is basically logging the
4 streams of data that are coming through it, correct?

5 A That are -- That are requests that are made to it, yes.

6 Q Okay, the requests that are made to it. And have you
7 looked at those streams of data before that are being logged?

8 A Yes, I have.

9 Q And how many times have you looked at streams of data
10 that are being logged from requests from peers on the law
11 enforcement nodes?

12 A Thousands since we started in 2012.

13 Q And what type of data in these requests are being logged
14 by the law enforcement node?

15 A We -- The only data we have, we have the IP address. We
16 have the date and time we saw it. We have the key that is
17 being requested, that SHA256 hash. We have the Hops To Live
18 value at the time. We have the number of peers that our node
19 -- that we received it from in the past. He'll tell us the
20 number of peers that he has.

21 Q And is the law enforcement node intercepting these
22 communications or how -- how does that work?

23 MR. FEIN: I'm going to object, Your Honor. That
24 calls for a conclusion, a legal conclusion.

25 THE COURT: Sustained.

1 Q (By Ms. Lang) The information that the law enforcement
2 node is collecting and logging, how is that information coming
3 to them?

4 A Well, we're a passive participant in the network. We're
5 the same as any other node in the network that will -- that
6 will process. So we get a request that's directed to us to
7 look for that -- that piece of material in our data store. If
8 we don't have it, we will generate a new message to one of our
9 peers to request it. We have to keep track of who made that
10 request so that when it comes back from one of our peers, we
11 know where to send it to because the only guy that knows the
12 IP address is only your directly-connected peer. You don't --
13 It doesn't get passed downstream as a request for this. So
14 when we receive that message, that's when we're involved.
15 It's a message that is directed to us.

16 Q And since *Freenet* is an open source program, any peer on
17 the -- on the *Freenet* program could begin to log this data,
18 correct?

19 A Anybody could modify it to do this, yes.

20 Q And we're talking about log -- The information you're
21 logging are the requests for files or blocks of files that are
22 coming from your peer. What's the difference between a
23 "requester" or a "relayer" of that information? Could you
24 explain that relationship?

25 A Sure. What we're interested in is who is originally

1 attempting to download this file. So the original requester
2 will send requests for blocks out to his peers. If those
3 peers don't have that block to return to him, they'll, in
4 turn, send a message to their peers asking for that same
5 block. And so what you have to -- What we have to try and
6 determine: Did we get that message from the original
7 requester or did we get that message from one -- one of the
8 Hops To Live?

9 Q So a relay.

10 A A relay.

11 Q And does the relay know that they might be passing on a
12 message for a block of child pornography?

13 A They wouldn't know based on the request.

14 Q I mean the law enforcement node knows because you guys
15 keep a database of known files, correct?

16 A It doesn't necessarily know at the time it received it at
17 the node itself. It wouldn't know.

18 Q Okay. But, obviously, the original requester knows what
19 they're requesting on the program --

20 A Yes.

21 Q -- because they have to paste -- Like we just went
22 through the whole example of how they have to find it and
23 paste it, correct?

24 A Correct.

25 Q And how does *Freenet* attempt to keep users anonymous?

1 A Well, it doesn't -- it doesn't actually try and keep the
2 user anonymous. We can clearly see what his IP address is.
3 What he tries to keep anonymous is what he's requesting under
4 the network, and it does that in a couple of ways. It tries
5 to -- to make it difficult to determine: Was that the
6 original requester or was that a relay? And then -- then it
7 -- You have to have some database to be able to even determine
8 what he's requesting. So they count on not knowing that
9 SHA256 hash belongs to child pornography.

10 Q So the basic method that law enforcement is using to find
11 requesters of child pornography on *Freenet* is to monitor the
12 requests that are passing through and looking at the -- if
13 this correct; correct me if I'm wrong -- and looking at the
14 number of requests that they're receiving, correct?

15 A Correct. We look at the number of requests that we've
16 received for a specific file relative to the number of peers
17 that the guy that sent it to us has and the size of the file;
18 the number of blocks that would have to be retrieved in order
19 to rebuild the file.

20 Q And looking at that information can differentiate
21 original requesters of the file versus relayers of just the
22 block of information.

23 A Yeah. The flaw in *Freenet* and Open Net is that there's
24 such a large difference in that next hop that the number of
25 requests will drop so dramatically between the original

1 requester and one relay out; that it's -- we can determine
2 that, based on the number, that we have a fair probability
3 that guy's the requester of the file.

4 Q And you know how -- And I'm assuming that law enforcement
5 knows how many blocks make up a particular file, correct?

6 A That's correct.

7 Q So like, for example, before you said if it was a
8 thousand blocks coming from -- that made up a file, then the
9 original requester would send out a thousand requests. And if
10 he had ten peers, they'd be divided up approximately a hundred
11 to each peer, correct?

12 A Correct.

13 Q So if a law enforcement node was one of those peers, they
14 would expect to see about a hundred requests from the original
15 requester.

16 A That's correct.

17 Q And if -- And if -- And to -- But if it was a relayer,
18 just one hop off, you would expect to see approximately ten.

19 A Right. You'd see a much -- much smaller.

20 Q Okay. Can law enforcement target a particular person on
21 *Freenet*?

22 A No, we can't.

23 Q And after you've determined that an IP address is the
24 original requester of a particular file, how do you verify
25 that that file is actually an image or video of child porn?

1 A Well, anytime we identify a file that -- *Freenet's* a
2 little different. The file names in a lot of cases are not
3 indicative of what the file is. So we'll download that file
4 and determine if it is, in fact, contraband; is it child
5 pornography. And we also want to do that to verify that the
6 complete file can be retrieved on *Freenet*; that it's -- that
7 the -- because it is possible that blocks have dropped out of
8 the network and that it's no longer downloadable.

9 Q And you're familiar with state and federal laws on what
10 constitutes child pornography.

11 A Yes, I am.

12 Q Now I'm going to move on to the investigation of this
13 particular Defendant, Mr. Dickerman. Back on April 2nd of
14 2015, was the law enforcement node running on *Freenet* or one
15 of the law enforcement nodes?

16 A Yes, there was. There were many.

17 Q Okay. And was there one particular one in Downtown
18 St. Louis that was running on April 2nd of 2015?

19 A Yes. Yes, there were.

20 Q And did that come across the Defendant's IP address?

21 A Yes, it did.

22 MS. LANG: Your Honor, I'm going to move on to
23 Exhibit 21 right now. May I show it to the witness?

24 THE COURT: Yes.

25 Q (By Ms. Lang) Investigator Becker, do you recognize

1 State -- Government's Exhibit 21?

2 A Yes, I do.

3 Q And what is it?

4 A That's a -- an Excel spreadsheet tool we developed to
5 summarize the data that we find on a particular target.

6 Q And that particular data goes to an IP address that's
7 listed at the top, starting with "172," correct?

8 A That's correct.

9 Q And was that the Defendant's IP address in this case?

10 A That's what the subpoena, yes, came back to.

11 Q And is that spreadsheet a fair and accurate
12 representation of what you were able to -- using the tools
13 that you have put together?

14 A Yes. Yes, it is.

15 MS. LANG: Your Honor, at this time I'd like to move
16 to admit Government's Exhibit 21.

17 THE COURT: Is there any objection?

18 MR. FEIN: No objection.

19 THE COURT: Exhibit 21 will be admitted into
20 evidence.

21 Q (By Ms. Lang) I'm going to swap out that one. That one
22 has a staple.

23 Investigator Becker, you said that this was the data
24 that was collected in reference to this particular IP address
25 on Freenet on April 2nd of 2015, correct?

1 A That's correct.

2 Q And this information was collected by a law enforcement
3 node which was numbered "693," correct?

4 A That's correct.

5 Q And that's there on the Exhibit 21, correct?

6 A That's correct.

7 Q And how is the data on this spreadsheet collected from
8 *Freenet*?

9 A The data -- The data that we collect from all the law
10 enforcement nodes goes into an ICAC database that an
11 investigator can look at that's -- that's sorted by their
12 regions. So they can look then in their jurisdiction. And
13 when they find a file listed in their jurisdiction that
14 appears to be -- meets our criteria at this time, then it
15 would -- they would copy and paste that data directly from
16 that ICAC website into this tool. So the idea with this tool
17 is to get that data off the screen so that you could then
18 manipulate it, analyze it and generate some numbers.

19 Q Okay. And how did this law enforcement node come across
20 this IP address on *Freenet*?

21 A It would have been connected to us. It would have been
22 one of our direct peers.

23 Q Because it had to be a direct peer in order for the law
24 enforcement node to know the IP address, correct?

25 A That's correct.

1 Q And there's a -- there's a file name, correct?

2 A Yes.

3 Q And did you verify that that file -- "Anonther Set 2" is
4 a ZIP file. Did you verify that that was, in fact, a file of
5 child pornography?

6 A Yes, I did.

7 Q And then listed under that is the SHA1 hash value.
8 What's that?

9 A That's the digital representation of -- a compressed
10 digital representation of that data. You can -- You can
11 generate a SHA1 hash for any kind of file, and that's --
12 that's kind of like a DNA or a thumbprint of that file.

13 Q So it's a -- it's unique to that particular file.

14 A Right. It's a unique identifier for that file.

15 Q And then two lines under that, it's listed "Data Block
16 783." What's that?

17 A This -- This -- That would be the minimum -- in this case
18 the minimum number of data blocks required to download the
19 file. Now *Freenet*, when it first inserts the file, actually
20 has a forward error correction system. There would be about
21 twice that many blocks stored. So if it can't find one, it
22 could find one of the others to rebuild it, but at a minimum,
23 it needs to find 783 to rebuild the file.

24 Q Okay. Then going below that, it says -- there's two
25 lines that say "First Block" and "Last Block Observed" with

1 the date and time. What does that reference?

2 A That would be the date and time stamps of the first block
3 we saw for that -- that file being requested from that IP and
4 the last -- the time of the last block we saw.

5 Q And then calculated below is the "Overall Run Time"?

6 A Correct.

7 Q And then there's "Average Peers," and it says "56.9."
8 What's that?

9 A That would be an average. Each record would have the
10 number of peers that this IP address is reporting that he had.
11 That's the average of those numbers. So he had probably 56 or
12 57, more closely 57 in order to get 56.9, but it just averages
13 it; simple average.

14 Q So this 56.9 is the average number of peers that this IP
15 address had, correct?

16 A That's correct.

17 Q And then it says "Percentage of Total" and then
18 "Percentage of Even Share." What are those numbers
19 referencing?

20 A The "Percentage of Total" is what percent of the total at
21 783 did this -- did we see; what percentage of the total
22 blocks for that file did my node see; --

23 Q Okay.

24 A -- receive the request for.

25 Q And what's "Percentage of Even Share" reflect?

1 A So we try and calculate that number. If I was trying to
2 get to a hundred, it would be about a hundred percent. So
3 we're looking to see did we get at least a hundred percent of
4 what we expected to get or better from that request; from
5 those requesters. That -- That gives us the good indication
6 that we've got the guy that's requesting the file. If it's
7 less than that, it could still be the guy requesting the file
8 but we typically don't use those. We want some level of
9 certainty.

10 Q And I noticed I missed a box. The "Total Unique Requests
11 Logged" in this case was 69.

12 A Correct.

13 Q And are those the requests that came from this IP
14 address?

15 A That's correct, where you see 69 requests.

16 Q So you -- So the law enforcement node received 69
17 requests for this file out of 783 minimum number of requests
18 that would have been sent out.

19 A Correct.

20 Q And then just on the last -- the "Frequency Group" which
21 has "10, 2, 1, 1, 4," could you just briefly explain what
22 those numbers are there for?

23 A That just tells us how many records we received in a
24 two-second period or three-second up to a six-second or more.
25 For example, in this case four times we received six requests

1 for this document. That just gives us a level of confidence
2 if we're close to that because the farther away you get, the
3 more hops away you get from there, the harder it's going to be
4 to get those kinds of turnaround numbers, but that varies
5 widely. It will vary depending on how many files he's been
6 currently downloading, where in the world we are in relation
7 geographically to that guy. So it's not by itself used for
8 anything.

9 Q So while the timing may not be a definitive that it's --
10 that he's the peer, it is some evidence that if it's a short
11 time, that he could possibly be a close peer.

12 A Yes. The confidence enhancer, if you will. We have to
13 hit the numbers first. We first have to have a big enough
14 number of requests for the file.

15 Q Okay. And speaking of that number, you said you're
16 looking for at least 100 percent or more of the Percentage of
17 Even Share of the requests. In this case it says it was 501
18 percent.

19 A Correct.

20 Q And so that's five times -- you saw almost five times the
21 number of requests that you expected to.

22 A Of the minimum number, and it could be twice that. He
23 could have needed to request closer to 1500 which would make
24 that two-and-a-half times of what we would expect to see, but
25 that's the range we would be falling into, yes.

1 Q And you saw -- And, again, you saw 69 requests from this
2 particular IP address that had to request at least 783.

3 A Yes.

4 Q So what do -- what do those numbers tell you as someone
5 who has been working on -- on *Freenet* looking for offenders
6 and original requesters?

7 A That that's what somebody downloading a file looks like.

8 Q So he had to have been, based on these numbers, more
9 likely than not the original requester.

10 A Correct.

11 Q And what evidence, just looking at the data that was
12 collected, do you use to differentiate that he was not just a
13 relay of this file?

14 A Can you ask that ---

15 Q Is there -- Is there any evidence that you look at to
16 determine -- You -- You said that you -- by looking at this, I
17 guess, that you believe he's a requester. Is there anything
18 you look at to determine that he's not a relay basically?
19 Any -- It's kind of the same question.

20 A What we look -- It's an either/or. It's a -- That's all
21 we need to determine is either he's a requester or he's not.
22 So that's -- So we determine, looking at those numbers, that
23 he's more likely the requester than a relay.

24 Q And then can you tell or do you remember: Were there any
25 duplicate file requests or any insert files in this particular

1 case?

2 A On this particular file there were two inserts. And I
3 mentioned how there's double the actual number of blocks,
4 roughly, because of this forward error recovery scheme,
5 *Freenet* users. Well, if he can't find a block but he finds a
6 different block that's he's able to rebuild a file, he'll heal
7 the file. He will insert that missing block when he's all
8 down; when he's rebuilt the file. So that's typically why we
9 see those extra insert blocks.

10 Q And so it was actually 71 requests but you took out the
11 two inserts before you did the math, correct?

12 A The math just based on the -- just based on the requests,
13 yes.

14 Q The unique requests.

15 A The unique requests. And the unique requests is the same
16 as the total requests in this case which means there were no
17 duplicate requests. If we started seeing duplicate requests,
18 that would indicate to us that he's having trouble finding a
19 block. There's maybe a missing block, and that will increase
20 the number of requests dramatically. So we use that as a
21 filter. If we see a lot of duplicates, we won't use the file.

22 Q Because that can skew the numbers?

23 A It can skew the numbers.

24 Q Now after you collected this information, whom did you
25 send it to?

1 A I originally sent it to Chris Mattei, the ICAC Commander
2 at the time.

3 Q And he was in the St. Charles office? Is that correct?

4 A Yes.

5 Q And did you also send information to Sergeant Kavanaugh
6 in the St. Louis County Police Department?

7 A Yeah, I did. Ultimately I did, yeah.

8 Q Now on this particular IP address, when you were doing
9 your investigations online on *Freenet*, did you ever come
10 across this particular IP address again?

11 A I came across this IP address in April and identified
12 three files in April that appeared to be downloading. And
13 then I did it again in June and created the information that I
14 ultimately sent to Adam Kavanaugh.

15 Q So how many times did you come across -- How many
16 different dates and times did you come across this IP address
17 requesting a file of known child pornography?

18 A That we documented in the tool, it would have been five
19 different files.

20 Q So five different files this -- this particular IP
21 address requested on *Freenet* that were known child pornography
22 files to law enforcement.

23 A That's correct, that we looked at. There was -- There
24 were many other files that were out there that we didn't
25 analyze.

1 Q I'm moving to Page 2 of Exhibit 21. There is another
2 file name there; same IP address listed in this spreadsheet.
3 Is that correct?

4 A That's correct.

5 Q And this one was also documented in the spreadsheet, and
6 why was that?

7 A This -- This -- There were -- For some reason there was a
8 delay when getting the subpoena back, so when that came back,
9 it did not come back till June. I again looked at this IP
10 address and discovered I was still seeing files being
11 downloaded that had a significant number of blocks and
12 identified two additional files.

13 Q So on -- on June 13th of 2015, the Defendant's IP address
14 again had a large number of requests for a child pornography
15 file going through the law enforcement node.

16 A That's correct.

17 Q And then -- Sorry. I missed -- I missed one because it
18 kind of goes on to two pages, but the bottom of Page 1 of
19 Exhibit 21 and then on to Page 2 there's a file of interest
20 listed as No. 2. Again, is that the same IP address?

21 A Yes.

22 Q I'm looking at Page 2 of Exhibit 21 at the top. That
23 was, it looks like, June 4th of 2015 that that was -- file was
24 recorded that the Defendant requested on the -- through the
25 law enforcement node.

1 A That's correct.

2 Q Now were you involved in the search warrants on the -- on
3 Alden Dickerman's house?

4 A Yes, I was.

5 Q And besides helping with the drafting of the search
6 warrant somewhat, you also were there when they executed the
7 search warrant with St. Louis County Police, correct?

8 A Correct.

9 Q And that was on, approximately, August 18th of 2015?

10 A Yes, ma'am.

11 Q And here in the Eastern District of Missouri was his --
12 where his home was located?

13 A Yes, it was.

14 Q And when you were at the scene, did you have an
15 opportunity to look at any computers that were in the
16 Defendant's -- that were the Defendant's?

17 A I don't believe I previewed any on-scene.

18 Q Did you end up doing the computer forensic analysis of
19 the Defendant's -- of the computers taken from the Defendant's
20 home?

21 A Yes, I did.

22 Q And did you determine whether there was any child
23 pornography located on his computers?

24 A Yes, I did.

25 Q And there was about 593 image files? Is that correct?

1 A That's correct.

2 Q And 42 unique child pornography video files.

3 A That's correct.

4 Q And he had a series of infants and toddlers, including
5 sadistic and masochistic activities in these.

6 A Yes, he did.

7 Q Now also of note in your computer forensic analysis you
8 saw that there was *Frost* subscription boards. What are those?

9 A *Frost*, as I think I mentioned earlier, it's a message
10 board that runs under *Freenet*. It's commonly used to exchange
11 keys to files related to child pornography. And you -- you
12 subscribe to a board, a message board, similar to the old
13 Usenet if you're familiar with the old Usenet system. You
14 subscribe to the board, and then you can post and retrieve
15 messages related to the board. He was subscribed to these
16 three boards, PTHC, Lolicam and HurtCore.

17 Q And would that be a place to find the keys to find child
18 pornography?

19 A Yeah. PTHC, which stands for "Preteen Hard Core," is the
20 most active board on *Frost*. Lolicam is typically where
21 they'll post cameras, captures of underage, and then HurtCore
22 is an S & M type -- type board.

23 Q And were these images of child pornography found in
24 allocated space on the Defendant's computers?

25 A Yes, they were.

1 Q And did you have an opportunity to see if he had any
2 *Freenet* browsing history on his computer?

3 A Yes, I did. I did examine the computer for browsing
4 history, and there were hundreds of references either to a
5 direct download of a file in the -- in the browser which you
6 can do on *Freenet* or to a free site that we noted contained
7 keys to child pornography.

8 MS. LANG: I don't have any further questions,
9 Your Honor.

10 THE COURT: Mr. Fein?

11 MR. FEIN: Thank you, Your Honor.

12 CROSS EXAMINATION

13 QUESTIONS BY MR. FEIN:

14 Q Good morning.

15 A Good morning.

16 Q I'd like to go back to September of 2011.

17 A Okay.

18 Q If I understand correctly, that's when you began to build
19 the database of keys, correct?

20 A That's correct. At that time it was a manifest of keys I
21 was collecting.

22 Q Tell me how you built that database.

23 A Originally that database was built completely manually.
24 Using the key-util facility that's built into *Freenet*, I could
25 look up -- Well, let me step back.

1 When I was collecting all the manifest keys, I would
2 just keep them in a text file of my own; kind of a running
3 list.

4 Q I'm sorry; forgive me. You were just using what?

5 A Manifest keys. Just the top level manifest keys that I'd
6 find off of free sites or off of *Frost*.

7 Q So I'll stop you there. So basically you're going to
8 free sites and you're looking for these keys, correct?

9 A Yeah. If you recall the example we had where they have
10 them listed at the bottom, you could copy and paste that whole
11 list of keys.

12 Q A key is an alphanumeric expression, correct?

13 A Correct.

14 Q And how many -- How long did it take you to build that
15 database?

16 A To get it to any significance -- Well, we -- Like I said,
17 we initially began in 2011 building just -- just manifest
18 keys. When we began logging records, which was not until
19 2012, I realized I needed more than the manifest keys. You
20 needed all those split keys associated with them.

21 Q So the question again is: How long did it take you to
22 collect those keys and build that database?

23 A It continues today. We do it continually.

24 Q Okay. And you -- How often do you engage in that
25 activity?

1 A Daily.

2 Q And you said "we." How many people along with you are
3 collecting keys?

4 A Early on there were some ICAC investigators up in
5 St. Charles that were manually -- when we were manually doing
6 it. By 2012 I had automated the process, and then we weren't
7 doing any --

8 Q So, again, the question is ---

9 A I didn't need them any longer to send me keys.

10 Q So the question is: How many people are logging these
11 keys?

12 A Finding the keys?

13 Q Correct.

14 A There may have been three total, including myself.

15 Q Is that here in Missouri?

16 A Yes.

17 Q Are there people collecting keys in other states?

18 A Not since 2012.

19 Q Not since when?

20 A Later in 2012 when I automated the process.

21 Q So before you automated the process, how many people were
22 assisting in collecting keys?

23 A Three.

24 Q Just three.

25 A Yes.

1 Q And that was here in Missouri?

2 A Yes.

3 Q People were not collecting keys in other states?

4 A Not that I -- No, I don't believe so; not then.

5 Q So let me -- Do you know if people were collecting keys
6 in other states?

7 MS. LANG: Objection; asked and answered.

8 THE COURT: Overruled.

9 A No, I don't.

10 Q (By Mr. Fein) Okay. How many keys were collected -- Let
11 me rephrase that because you've indicated that you continue to
12 collect keys.

13 To date, how many keys have been collected?

14 A The last count I had, we had about 75,000 manifest keys
15 and then 170 million split keys.

16 Q I'm sorry. 170 million what?

17 A Split keys.

18 Q Split keys?

19 A Yeah; the key to those individual blocks that make up a
20 file.

21 Q Just to clarify something, I think you actually clarified
22 it yourself but just to make sure it's right for the record:
23 Earlier you said -- you testified that IP addresses are
24 exposed, correct? You had said that at some point?

25 A Sure, yeah.

1 Q But the IP addresses that are exposed to a particular
2 user are those of the user's peers, correct?

3 A Yes.

4 Q The IP addresses of nonpeers are not exposed to a user.

5 A They could be.

6 Q That's not my question. They could be, but they're not,
7 right? You have to go through some steps to make them -- to
8 expose them, correct?

9 A No. There's a display of Internet connections built into
10 *Freenet* that are -- include IP addresses that are no longer
11 your peers.

12 Q I understand. So -- But if they were never a peer of
13 yours, --

14 A You wouldn't have never seen it.

15 Q -- you would not have seen it, right? Correct?

16 A That is correct.

17 Q So either they're a current peer or a former peer.

18 A Or they were, yeah.

19 Q Otherwise, you would not have an exposed IP address.

20 A That's correct.

21 Q The keys that you collected to build the database were
22 gathered from free sites. Those free sites could be located
23 anywhere in the country, right? On a server anywhere in the
24 country on a computer?

25 A They're -- They're not on a server.

1 Q Forgive me.

2 A They're -- They're scattered all over just like ---

3 Q Right. They're on *Freenet* users' computers, correct?

4 A Correct, yes.

5 Q And they could be anywhere in the country, correct?

6 A Anywhere in the world.

7 Q Do you know how many people around the world use *Freenet*?

8 A I've seen various statistics over time.

9 Q I'm asking you if you know personally --

10 A No, I don't.

11 Q -- how many people. Do you know personally how many
12 people in the country use *Freenet*?

13 A I do not.

14 Q Do you know how many files are stored on *Freenet*?

15 A I do not.

16 Q Just to run through a couple of small steps, the first
17 step in your process beginning in September of 2011 was
18 collecting keys, right?

19 A Yes.

20 Q Those keys would lead you to a manifest, correct?

21 A Correct.

22 Q The manifest operates like a Table of Contents, correct?

23 A Correct.

24 Q It gives you the blocks that are needed to complete a
25 file, correct?

1 A That's correct.

2 Q The blocks to these files are hashed, right? There's a
3 hash value assigned to each block?

4 A That's correct.

5 Q A hash value is an alphanumeric expression that's unique
6 to a given static file, unchanged file, correct?

7 A That's correct.

8 Q It could be an audio file?

9 A It could be any kind of file.

10 Q It could be a text file; could be a digital file.

11 A Yes.

12 Q To create the database, you had to know that the keys you
13 were collecting that led to the manifest that led to the
14 blocks were, in fact, related to child pornography, correct?

15 A That's correct.

16 Q How did you make that determination?

17 A Well, we -- Either visually early on, but as we -- as it
18 grew to where we didn't have the ability to download all those
19 files, we did it by obtaining them from on-topic free sites or
20 on-topic message boards.

21 Q So when you said "we did it by" ---

22 A And I'm saying "we." I did it by getting them from free
23 sites or on-topic message boards.

24 Q So you would look at the images, correct?

25 A Not necessarily.

1 Q So if all you have is a hash value or all you have is
2 some data, how do you know that that relates to child
3 pornography?

4 A We -- We -- Because we obtained it from a source, such as
5 a free site like the example we saw, or we got it off of a
6 message board that -- that was dedicated to that type of
7 material.

8 Q At some point you had to look at it, right?

9 A Yes, we would. We would look at it when we determined,
10 "Hey, we think we have somebody that's downloading this file;
11 what is the file?" And there's two reasons we have to do
12 that.

13 Q Well, I understand, but I'm just curious about building
14 this database right now.

15 A Yes, at some point we had to look at the files.

16 Q So what happened to the files you looked at? Were they
17 copied onto the system you were using?

18 A Yeah. They were added to a nodable library in my case.

19 Q Okay.

20 A I can't speak for every investigator. In my case they
21 were added to a nodable library.

22 Q Does that library still exist today?

23 A Yes, it does.

24 Q Okay. So there's a library that contains all these
25 images, whether visual -- whether still images or videos, a

1 library that contains these images of child pornography.

2 A Yes. That's not an exclusive library to *Freenet*. That's
3 from cases I've worked over the years from many sources.

4 Q Who operates that system --

5 A I do.

6 Q -- or that database? Forgive me.

7 A I do.

8 Q You have that?

9 A Yeah.

10 Q Okay. And once you've identified a particular instance
11 of child pornography, a file of child pornography and you've
12 associated that file with blocks and hash values that comprise
13 that file, then ultimately when you're looking at the blocks
14 of another file by comparing the hash value, you can know what
15 matches with that file that you've already included in your
16 database. Is that a fair statement?

17 A I think. Yeah, if I understand your question.

18 Q And forgive me. I'm not the most technologically
19 sophisticated individual.

20 Once you've identified the files consisting of child
21 pornography, once you've identified the hash values associated
22 with the blocks that comprise it, then in future instances you
23 do not need to view the image again. You view the hash value,
24 and that tells you it's a match, and you know it's consistent
25 with child pornography already logged in your database. Is

1 that fair?

2 A No, that's not exactly what we do.

3 Q So tell me about what you actually do.

4 A We would down -- We would download it again. I may look
5 to see, yes, this is a child pornography file because I've
6 already seen it, but I might have seen it last year or so far
7 back. I want to download it again to make certain that I can
8 still retrieve that file from *Freenet*.

9 Q So let me do it in this way, too, just to make sure we're
10 on the same page. Suppose there was an investigation. This
11 was an investigation of me --

12 A Okay.

13 Q -- and you downloaded some rather -- Forgive me. Let's
14 keep it with *Freenet*.

15 You had determined or made a statistical analysis
16 that suggested I was the requester of a file, and you had the
17 blocks that comprise that file and you had the hash values
18 associated with that file. Would you then go and check your
19 database and look at the actual image again or would you
20 simply make the assumption that based on those hash values,
21 it's a known instance of child pornography?

22 A No. I would check the database to see what the file
23 really was.

24 Q Okay. So you'll get the hash values associated with the
25 blocks, and then you'll double-check and you'll actually look

1 in your database to make sure it is, in fact, an instance of
2 child pornography.

3 A And then I'd go one step further. I would download the
4 file again from *Freenet*.

5 Q Okay. Where would you download the file from?

6 A *Freenet*.

7 Q Okay. So you would actually look at the -- You would get
8 the hash values that would suggest the content. You'd confirm
9 the content through your database, and then you would again go
10 and get the file from *Freenet* and double-check that, again
11 looking at the content, making sure it's child pornography.

12 A That's correct.

13 Q Okay. And the data -- Do you have a separate database of
14 hash values and a database of images? There are two separate
15 databases?

16 A I believe so, yes.

17 Q All right. Who maintains the database of hash values?

18 A ICAC does.

19 Q Where do you maintain these database?

20 A You know, I don't actually know for certain.
21 Pennsylvania someplace. To be honest with you, I don't know,
22 sir.

23 Q Who -- Are you the only contributor to this database?

24 A Of keys?

25 Q Yes.

1 A Yes.

2 Q What other information is contained in that database?

3 A It would be the manifest key and then all the associated
4 SHA256 hash that make up the files of that manifest. And then
5 there's metadata or data in the manifest that we'll collect
6 what the SHA values of the actual file are. There's SHA256,
7 SHA1, whatever is contained in their, the size of the file,
8 information such as that.

9 Q Who contributes to that?

10 A I do.

11 Q Are you the only individual who contributes all that
12 data?

13 A Yes.

14 Q There's no other individual involved in constructing that
15 database.

16 A No. It's somebody -- somebody on the other end. I -- I
17 forward that data. I pull the data out of *Freenet*, put it in
18 a -- put it in a common format every day, and then send it to
19 somebody who has the process that adds it to the database.

20 Q What's the name of the -- Is there -- Is this an
21 institution? Is this an individual that's working with you?
22 Another law enforcement officer?

23 A No. It's a scientist at the University of Massachusetts
24 - Amherst is my direct contact. So if I have a problem or it
25 was broken or something along those lines, that's how I

1 contact them. I think the whole process is very automated.
2 It's automated on my end. You know, I don't -- I don't have
3 to touch it unless there's some kind of problem.

4 Q So for example, perhaps the expert who's testifying for
5 the Government today might be maintaining that database.

6 A Yes, could be.

7 Q All right. And, again, that process began in September
8 of 2011, and this is just the process of collecting keys and
9 data. This began in September of 2011 and continues to this
10 day.

11 A Yeah. The database that we're updating now didn't exist
12 then, but that's what it evolved into.

13 Q Okay. And you said that it's automated at this point,
14 and tell me about that automation process.

15 A I've got a program that -- that looks at the *Frost*
16 system, the messaging system, every night for new people that
17 have posted new messages, new keys to files, and I look at
18 specific on-topic boards. And then we'll look those keys up,
19 using *Freenet*'s own facilities, look up all the associated
20 keys and the metadata associated with that file to build our
21 records that we then load to the database.

22 Q Okay. And that particular database just has keys, hash
23 values, these various symbolic expressions, right? These
24 alphanumeric expressions?

25 A Yes. They don't have any images or -- or any data file,

1 anything of the data itself.

2 Q I mean the alphanumeric expressions are data, too, right?

3 A Yeah. It doesn't have the actual -- what they

4 represent, --

5 Q The visual depictions.

6 A -- the visual images or videos.

7 Q Just has keys, the manifest likely, --

8 A Yes.

9 Q -- blocks and the hash values that are associated with
10 them.

11 A Yes, sir.

12 Q Okay. You maintain the images.

13 A Not just me. I mean I maintain images on cases I work.
14 Officers working *Freenet* cases other places would do the same
15 thing.

16 Q And do you have access to those databases?

17 A I do not.

18 Q So when you conduct an investigation, you'll only be
19 comparing your work to your own database of images.

20 A If I had it already. If I didn't have it already, like I
21 just said earlier, I'd download it from *Freenet* to see what it
22 is.

23 Q Fair enough. Let's go to April of 2012. And if I
24 understand you correctly, in April of 2012 you began running
25 *Freenet*, correct?

1 A Yes. We began logging -- We began running a version of
2 *Freenet* that would log the requests, that's correct.

3 Q Okay. So again you say "we." Who is "we"?

4 A I keep saying "we." I'm referring to myself at this
5 point in time. Nobody else is doing it at this point.

6 Q Okay. And so to do this, you've downloaded *Freenet*?

7 A Correct.

8 Q Was this version of *Freenet* modified?

9 A Yes.

10 Q Who was it modified by?

11 A Dr. Marc Liberatore with the University of Massachusetts
12 - Amherst created a patch to log those records for me.

13 Q What's a "patch"?

14 A A modification to that source code so that the program
15 would -- would write these records.

16 Q So it's a program that what? Forgive me.

17 A Would write out those log records; would log the requests
18 for these things.

19 Q Okay. So you didn't download *Freenet* from the *Freenet*
20 site. You received this piece of software from an individual
21 at the University of Amherst.

22 A I -- I didn't download the runnable like -- as we showed
23 you how somebody would install it. I downloaded the source
24 code from -- from *Freenet*.

25 Q And what did you do with the source code?

1 A I applied the patch that Marc Liberatore provided me and
2 recompiled *Freenet*.

3 Q So, again -- So you had the source code. It was modified
4 by the University of Amherst. That modification allowed for
5 logging, correct?

6 A Correct.

7 Q Okay. That logging allowed you to log what?

8 A Whatever requests were received by -- by a node I was
9 running.

10 Q Okay. That's a little abstract. What's the data that
11 it's logging?

12 A With a request, what the data was logging would be the
13 date and time, the IP address, the SHA256 hash of the key that
14 was being requested or inserted, whether it was a request or
15 an insert; log the port number which is a part of the
16 networking side of things; would log the Hops To Live value.

17 Q And at this point in time in April of 2012, are you the
18 only law enforcement officer doing this to the best of your
19 knowledge or are there others that you know of?

20 A Just myself to my knowledge.

21 Q Okay. And the logging process, the modification that
22 allows you to engage in the log-in, is that automated?

23 A It was not then. Those were -- It would create a text
24 file. I'd have to manually shut down *Freenet* and start it up
25 again to cause that file to be cut off so that then I could do

1 something with it. So it was -- it was somewhat manual.

2 Q Okay. So explain to me that process.

3 A So the -- When you started *Freenet*, this logging function
4 just -- it was just -- any request it received, it wrote it
5 out to a text file.

6 Q Let me just stop you right there. How many -- How often
7 would you be doing this? Would you be sitting in front of a
8 computer all day long?

9 A Some days. Ultimately what I did is I -- I created a
10 script for these systems running it that would automatically
11 stop *Freenet* once -- once a day or twice a day and start it
12 again which would cut off that log file, and then I could do
13 something with that log file. But until I did that, I
14 couldn't actually do anything with that.

15 Q So let's talk about before you did that. All right? So
16 let's talk about before you had the script and you're just --
17 It sounds like you're acting on your own, doing a manual
18 process.

19 A Yes, pretty much.

20 Q What timeframe are we talking about?

21 A This would have been late 2012. From about the Summer of
22 2012 till late 2013.

23 Q Okay. I thought you started in April of 2012.

24 A I got the patch in April of 2012.

25 Q Okay. But the actual logging process began around the

1 Summer of 2012?

2 A Well, I had to create nodes and start them up, so it was
3 summer, June.

4 Q Okay.

5 A It was probably May/June that I starting running nodes,
6 collecting data.

7 Q And so this manual process ran through the Summer of 2012
8 till when?

9 A The Fall of 2013.

10 Q And describe to me this manual process.

11 A I would -- I would have to stop the *Freenet* node that was
12 collecting the data.

13 Q Let me stop you even there. So, again, I'm not very
14 sophisticated. So I'm assuming you're sitting in front of a
15 terminal. You're sitting in front of a computer.

16 A Running *Freenet*.

17 Q Okay.

18 A I'm on the screen -- some of the screens we saw earlier.
19 I stop. There's a stop command to stop *Freenet* which causes
20 it to close that file. It was a very simplistic patch to
21 write this log file. There was no mechanism to cut it off or
22 send the records automatically to anybody. It just created
23 this file. And then I'd start *Freenet* again and start a new
24 file. And I could take the previous one that just cut off,
25 copy it to wherever I was going to manipulate it.

1 Q So let me stop you there. So each time the software
2 would stop, you would have to log something manually.

3 A It would close the file. I didn't have to do it. The
4 program would close the file when you stopped it.

5 Q Okay. Once it stops, what are you looking at?

6 A A list -- Basically a text file separated by commas with
7 those fields I mentioned earlier; the HTL, the IP address,
8 et cetera.

9 Q How many addresses would be listed?

10 A Thousands and thousands.

11 Q How many thousands?

12 A Hundreds of thousands ultimately. I mean depending on
13 how often I cut it off, I might have a node to generate 10,000
14 requests or if I cut it off daily, it might be 100,000
15 requests or 200,000 requests. And then if I had multiple
16 nodes, you're going to be adding all that data together and
17 maybe looking at millions of records on a single day.

18 Q So hang on. Were there multiple nodes -- Were there
19 multiple -- Let's try to use the word "computer." I know
20 "node" is the word *Freenet* users like to use but just to keep
21 things simple.

22 A Sure.

23 Q How many computers would be running *Freenet* for you at
24 that point in time?

25 A I started with one, and we built -- I probably had eight

1 at one time.

2 Q So let's step back and just keep it to the timeframe I'm
3 trying to focus on at the moment which is Summer of 2012 to
4 Fall of 2013. How many computers operating *Freenet* did you
5 have at that time? During that timeframe.

6 A From one to eight.

7 Q From one to eight. And each one of those computers
8 running *Freenet* modified would automatically cut off, correct?
9 So you -- So that the information could be logged.

10 A Yeah. What -- What I ended up doing was developing a new
11 script. To stop and start *Freenet* still causes the file to be
12 cut off.

13 Q And each time it stopped, there could be thousands of IP
14 addresses listed.

15 A Yes. Not -- Yes. There could be thousands of IP
16 addresses, thousands of records logged.

17 Q Right.

18 A So each one of those -- each one of those log records was
19 an individual request that my node received.

20 Q Okay. So there could be thousands, and each instance of
21 one of those thousands is a request from some user of *Freenet*.

22 A Correct.

23 Q How often would they stop? How often did the program
24 stop in a given day?

25 A Generally once.

1 Q How often did you stop the program? Once a day? Twice a
2 week?

3 A Once a day. Every -- Every night like at midnight it
4 would -- the script would stop and start. So it would cut the
5 file off once a day.

6 Q Okay. So between Fall of -- Forgive me. Yeah. Between
7 Summer of 2012 and Fall of 2013, you ran between one and three
8 computers operating modified *Freenet*.

9 A Between one and eight.

10 Q Forgive me; between one and eight.

11 A Yes.

12 Q Thank you. The modification was designed to stop the
13 running of *Freenet* every night at midnight you said.

14 A The script was.

15 Q The script.

16 A Yes.

17 Q Every night at midnight there would then be thousands of
18 IP addresses or thousands of requests that were logged.

19 A That's correct.

20 Q That logging progress was automated. You didn't have to
21 log, write down all those IP addresses by hand, right?

22 A No.

23 Q All right. Okay. So the -- Let's just assume for a
24 moment that this did take place every night at midnight. So
25 each night would you review it at midnight?

1 A No. I would -- The data would be -- Depending on where
2 the node was, if it wasn't right there in my office, I'd have
3 to transmit that data in --

4 Q Okay.

5 A -- to me so that I could -- I would have it in my office.

6 Q Okay. Where might the node be?

7 A Other law enforcement agencies across Missouri. At that
8 time I was using some old Pentium laptops that ICAC used to
9 use as training devices, and that's what I built those nodes
10 on.

11 Q Okay. And that would be between one and eight of those
12 running.

13 A Right. And then who -- whatever agency would give me
14 some bandwidth --

15 Q Okay.

16 A -- to run one of those nodes.

17 Q So every night at midnight it stops. The next day you
18 come in because presumably you need to sleep.

19 A Yeah.

20 Q And you go through the data.

21 A Yeah. The data overnight would have been sent in to my
22 facility, and then I would have merged it all up and loaded it
23 into a database.

24 Q Okay. So every day you come into the office and from the
25 preceding night there are thousands of logged entries.

1 A Correct.

2 Q What do you do with those logged entries?

3 A I'd look at the ones that occurred in Missouri. Part of
4 that nightly process when I looked at an IP, I would look it
5 up using -- We had bought a service from *MaxMind* which is one
6 of various services that will provide an approximate
7 geolocation for an IP address, and that's a publicly-available
8 service. They're happy to take your money. And so I'd look
9 those IP addresses up and see if -- and then put where *MaxMind*
10 thought they were.

11 Q So let me stop you there. So we've got every day
12 thousands of these things. I'm going to make an assumption
13 -- tell me if I'm right or wrong -- that that process, again,
14 is automated.

15 A Yes.

16 Q You're not visually looking at each little one.

17 A No.

18 Q Okay. So tell me about this automated process. How does
19 that function?

20 A Well, I take all those text records; you know, those
21 simple text files that I received from all those nodes every
22 night.

23 Q Well, hang on. Let's -- Let's focus on -- You said that
24 there was multiple pieces of data. There's an IP address,
25 right?

1 A Right.

2 Q The Hops To Live value, right?

3 A Right.

4 Q There's a date and time stamp?

5 A Yes.

6 Q There are hash values?

7 A A hash value, yes.

8 Q Right, okay. So how does this automated process work
9 with respect to those pieces of data?

10 A Well, I wrote a program that took those, that raw data,
11 and loaded it into a SQLite database. In the process of doing
12 that, I would add something. I would look up the geolocation
13 of that -- of that IP address; add that to the record.

14 Q Okay. So -- And when you looked for the geolocation of
15 the IP address, I take it likely what you're interested in is
16 where is that IP address likely located physically; to what
17 location is it connected.

18 A Exactly.

19 Q You're not interested in the computer user who's
20 downloaded *Freenet* and happens to live in Alberta, Canada.

21 A No. I was interested in the State of Missouri.

22 Q Right. So you have an automated process that starts to
23 filter out the IP addresses that are located in Missouri or
24 likely located in Missouri from those that are not.

25 A Yes. You could look up by that region any region you

1 wanted, but, yeah, we kept -- we kept all of it.

2 Q Okay.

3 A You could look it up by region.

4 Q You say "we." Who do you mean?

5 A "We," I'm still talking about myself.

6 Q Okay.

7 A It's the royal "me."

8 Q It's the royal "me." I have that same problem sometimes.

9 Okay. So this is an automated process, and it
10 separates out those IP addresses, correct?

11 A That's correct.

12 Q And that's going to be done every day.

13 A Yes.

14 Q Okay. Out of the -- Just to be clear, we've been saying
15 thousands every day. You said it could be 10,000. It could
16 be 100,000?

17 A It could be millions.

18 Q Okay. And at that point in time these are just users of
19 *Freenet*, right?

20 A Yes.

21 Q The content of their request, the content of the
22 information they're looking for is unknown to you at this
23 point in time. It's just a ---

24 A Well now, let me -- let me step back. Part of that
25 nightly process was also to look up that key, that SHA256, and

1 see if it was in my database of what we suspected to be child
2 pornography files.

3 Q Okay. So the log that you have, and it has the IP
4 address, has the date and time stamp, the Hops To Live value,
5 also has these hash values, ---

6 A Has the SHA256 hash of the block that's being requested.

7 Q And so the automated process not only segregates -- Well,
8 let me step back.

9 When you come in in the morning, before you run the
10 process to separate out the IP addresses based on geolocation,
11 does the software that you have modified already only log hash
12 values that are associated with child pornography already?

13 A Yes.

14 Q Okay. So you have -- So there's -- So the modification
15 that you have installed that is running every day and stops
16 every night at midnight is capturing all sorts of datastreams
17 from *Freenet*, correct?

18 A Correct.

19 Q And it is separating out through hash values only those
20 that have hash values associated, as far as you know or as far
21 as your database tells, with child pornography and excluding
22 those that do not.

23 A The patch that logged the raw data didn't have the
24 capability of making that determination. That determination
25 was made in -- in the back office, if you will, when I

1 received that and processed that raw data. We would only keep
2 those --

3 Q Okay. So let me take a step ---

4 A -- records that matched our database of what we suspected
5 was child pornography.

6 Q Okay. I think I got you. Let me take a step back.

7 So, again, everything is logged, thousands and
8 thousands of logs, and you have to determine at some point
9 whether or not what's logged relates to child pornography
10 through a hash value or not, right?

11 A That's correct.

12 Q That's done after the original logging takes place.

13 A Yes. We -- We process that log and only save what may be
14 child pornography.

15 Q So back to our -- When you come in the morning,
16 everything that's included in the log would include some that
17 do relate to child pornography based on hash value
18 determinations and some that do not, and you're going to
19 subsequently separate those out.

20 A Yeah. But that process -- I didn't do that process. I
21 wrote a program that does that process.

22 Q It was automated, --

23 A Yes.

24 Q -- right?

25 Okay. It's capturing all those datastreams, right?

1 And then the next day, after it stops and you come
2 in, through an automated process it's going to separate out
3 those that connect with hash values that relate to child
4 pornography from those that do not.

5 A Correct.

6 Q Then it's also going to separate out data that relates to
7 IP addresses within the State of Missouri, hopefully, from
8 those that are not.

9 A Yes.

10 Q And this is between the Summer of 2012 and the Fall of
11 2013; that was the process that was used.

12 A Yes.

13 Q Before the automated process separates out the logged
14 data that includes hash values that both do and do not -- Let
15 me restart that question.

16 The logged data that you come in and view each
17 morning then simply contains a list of *Freenet* users who've
18 made requests passing through your nodes.

19 A What I would review would be *Freenet* users that made
20 requests for child pornography.

21 Q Before you review it, when you come in in the morning,
22 before you've reviewed a thing, it's just a series of requests
23 from *Freenet* users for various material, along with their IP
24 addresses, their Hops To Live value, a date and time stamp and
25 hash values.

1 A I would never actually -- You mean did I personally look
2 at that data?

3 Q No, I'm not asking you if you looked at it. I'm saying
4 that's what would have been automatically stored by the patch
5 modified, --

6 A Yes. Okay. I'm sorry, yes.

7 Q -- right?

8 I think it would be very hard to look manually at
9 thousands and thousands of all this stuff. So just to be
10 clear, the modified version would store all that data; simply
11 requests made by *Freenet* users.

12 A Correct.

13 Q Then each day when you come in, the segregation process
14 starts.

15 A Well, we do it automatically overnight.

16 Q Okay. Forgive me.

17 A So it was done when I came in.

18 Q Okay. That's fine. So at some point that segregation
19 process starts. IP addresses are segregated out, and those
20 instances that involve hash values related to child
21 pornography are included. And through an automated process,
22 the other data is excluded that does not relate to hash values
23 associated with child pornography?

24 A Yeah. We take that raw file that came in from that.

25 Q Yep.

1 A And it would read a record; process, you know, its
2 geolocation, look up that SHA value and see if we thought it
3 was a child pornography file. If it wasn't, we just move on
4 to the next.

5 Q So, again, when you say "we," do you mean you?

6 A That would be me.

7 Q Or do you mean ---

8 A Or I mean the program. I'm probably talking about a
9 computer by now that's sitting there doing that every night
10 for me.

11 Q And it's easy to confuse individuals with computers. I
12 understand that. Was it really you or was it the University
13 of Amherst that's doing that component?

14 A At this point it was me. Those are all programs I wrote.

15 Q Okay. So when you say that you would -- or when I say
16 that you would segregate this data and keep that which was
17 relevant to you and exclude that which was not, tell me about
18 the exclusion process. What are you doing there?

19 MS. LANG: Objection; relevance to this line of
20 questioning with the suppression issues in this case.

21 MR. FEIN: Your Honor, ---

22 THE COURT: Yeah. Where are you going with that?

23 MR. FEIN: So here's one point I'm trying to make.
24 It strikes me that the Government is engaged in a process of
25 bulk collection of data from individuals around the country

1 simply using *Freenet* software; whether or not that bulk
2 collection of data and what they do with that data is relevant
3 for Fourth Amendment purposes because it may suggest that
4 there was a search going on nationwide for data associated
5 with *Freenet* users that is not subjected to any judicial
6 oversight. So I'm very curious about the data that is -- that
7 the Government claims is excluded from the process of further
8 what I would call a "search;" what happens to that data. If
9 that is innocent *Freenet* users potentially, where is that data
10 going?

11 MS. LANG: Your Honor, I don't -- First of all, I
12 don't think this is -- I don't think this is relevant to this
13 particular hearing. Mr. Dickerman has no standing to
14 challenge that. He was not caught on *Freenet* until 2015 which
15 the version we're talking about now of how things were
16 collected was back in 2012 and early 2013. So what -- I think
17 this whole line of questioning is improper. He has no
18 standing to challenge this at this point.

19 MR. FEIN: So Mr. Dickerman has been subjected to
20 this process, and I would argue he does have standing. He's
21 here in court today.

22 Further, it is ironic to me that when -- in an age
23 when the Government wants more and more transparency of the
24 citizens, there's less and less for the Government. I'm
25 simply asking if he is logging this data, and he's telling me

1 himself that it's excluded from the database. Where does it
2 go? I'm not asking him to identify ---

3 THE COURT: Is that the extent of your question?

4 MR. FEIN: That's it. Yes.

5 THE COURT: Okay. I will overrule the objection.
6 I'll allow that question.

7 A So -- So where are these raw data files? The original
8 raw data files? Is that your question?

9 Q (By Mr. Fein) The original raw data files that are
10 excluded because they did not contain hash values of interest
11 to you. Where do they go?

12 A We didn't do anything with them. I mean they -- they're
13 probably still on a file server in my office, but that would
14 be the extent of it.

15 Q Very good. That was the only -- They're on file
16 somewhere in your office.

17 A I don't believe I deleted them, no.

18 Q Very good.

19 So let's talk about the process from the Fall of 2013
20 forward. And before we start down that road, let me ask you:
21 How many changes have been made from 2013, the Fall of 2013,
22 to today?

23 A Changes to?

24 Q So for example, the process we just talked about was only
25 a process in use for a small period of time.

1 A Yes. It was a proof-of-concept kind of a project. It
2 was a small project that was run out of my office, yes.

3 Q Right. So what I'm getting at is: Did that -- The next
4 segment of time I'd like to talk about: Was there just one
5 process from the Fall of 2013 to today or were there processes
6 that were, again, changed over time?

7 A I'm sure they were changed over time. I don't think I
8 shut off what I was doing in the Fall of 2013, but we began
9 doing something different with ICAC in the Fall of 2013.

10 Q So I'm a little confused. The process that you used
11 between the Summer of 2012 and the Fall of 2013, that process
12 is still being used or not?

13 A No, it's no longer being used today.

14 Q Right, okay.

15 A It might have ran through most of 2014, but we had ceased
16 using it primarily.

17 Q Okay. So let me ask you this: So what is the process
18 that takes place come the Fall of 2013 or let's say the winter
19 of 2013?

20 A Okay. We got -- I got support or the project got support
21 from, I believe, the FBI. And I'm not the expert to answer
22 where the support came from, but the University of
23 Massachusetts - Amherst got involved with my project.

24 Q I'm sorry. I'm having a small trouble hearing with my
25 ears. The University of Amherst got ---

1 A The University of Massachusetts - Amherst, which we
2 typically just refer to as "Amherst," ---

3 Q Yeah. And they got support from whom?

4 A I believe they got a grant or they get supported through,
5 I believe, the Department of Justice or the FBI for various
6 projects.

7 Q Okay.

8 A But I'm not -- I'm probably not the one to ask exactly
9 how that support came about to look into *Freenet*. And so they
10 contacted me, knowing what I was already doing, and I began
11 working with them in the Fall of 2013.

12 Q Right. Well, if I understand it, you were working with
13 an individual at the University of Amherst before the Fall of
14 2013.

15 A Well, he had created a patch. That's why they knew about
16 me in --

17 Q Right.

18 A -- back in 2012. Then I continued on from that. I
19 wasn't using -- Nobody from Amherst was assisting in that
20 year, about a year time, not until the Fall of 2013.

21 Q Okay. But there was an individual at the University of
22 Amherst that had modified the original law enforcement *Freenet*
23 for you. He patched it, right?

24 A Right. He had created that patch for me.

25 Q That was in his own individual capacity? Is that what

1 you're ---

2 A No. I'm sure it was in his capacity as supporting ICAC.

3 Q Okay. But the institution began to support you in
4 December or the Fall of -- forgive me -- the Winter of 2013
5 through a grant proposal?

6 A Yeah. I'm not sure how it was funded.

7 Q Okay.

8 A But, yes, something like that. Anyway, I got -- I got
9 support that somebody began working --

10 Q Fair enough.

11 A -- to productionalize a little more --

12 Q Okay.

13 A -- the process I was using.

14 Q Okay. And more important to me, frankly, is that: At
15 that point what is the process at that point? How is it
16 different from the process we just discussed?

17 A Well, primarily, the primary difference is rather than
18 this batch logging every night where I get a big file that has
19 to be transferred, they created a version that does a realtime
20 transfer to the ICAC system. And so that record, when it's
21 received now, going back to your other point, they look and
22 say, "Is this -- Do we think we know what this file is?"
23 "Yes, we do," it goes into the database. "No, we don't," it
24 gets thrown away.

25 Q Okay. So that process -- So when you say it gets thrown

1 out, what do you mean?

2 A That means it's not recorded anyplace. It's not saved.

3 Q Do you know that for a fact?

4 A I've been told that.

5 Q You've been told. So you don't know that for a fact.

6 A I don't, yeah. I've been told that's how it works.

7 Q Okay. All right. Stick with what -- If you don't
8 mind -- I don't mean this personally.

9 A Sure.

10 Q Just stick with what you have firsthand information on.

11 Other than that, is there any change to the process?

12 A The process now moved to ICAC.

13 Q So -- Forgive me. That's poorly phrased.

14 So we discussed the 2012 to 2013 process. You just
15 told me about how now, moving from the Winter of 2013 on, that
16 there was some automation introduced into the process.

17 A Right.

18 Q And one thing that automation does is it segregates out
19 files of interest, based on hash values, from files of
20 noninterest; correct?

21 A Correct.

22 Q So that's one change. Are there other changes to the
23 process?

24 A I mentioned there was realtime. So we're recording in
25 realtime those -- those records to ICAC.

1 Q Okay. So ---

2 A And now that's -- that's the database that we retrieve
3 from.

4 Q Okay. And, again, how -- So, again, on each day are
5 there thousands of files coming through?

6 A Yes.

7 Q Okay. And those files are logged but they're logged now
8 in an automated way that segregates out at the outset files
9 that seem like they might be of interest from files that might
10 not be of interest.

11 A That's correct.

12 Q Okay. And they're still logging all the IP addresses.

13 A If -- If they have a file of interest.

14 Q Correct, right. So right now I'm assuming, moving from
15 the Winter of 2013 forward, that there's a database, and that
16 database only has files of hash values in which you have an
17 interest. Okay?

18 A Yes.

19 Q Okay. And with respect to those, it's logging all these
20 IP addresses.

21 A That's correct.

22 Q Okay. And, again, there's going to be thousands and
23 thousands of IP addresses every day.

24 A Yes.

25 Q And these are the IP addresses of individuals who have

1 downloaded and are using *Freenet*, correct?

2 A That had a file of interest.

3 Q Well, not really. That were -- Here's one thing that
4 we've already talked about; you talked about on your Direct.
5 They're connected maybe to a file of interest, but you don't
6 know yet at that point whether or not they are a requester of
7 that file of interest, --

8 A Okay.

9 Q -- right?

10 A Yes.

11 Q So it's just an IP address that has routed a file of
12 interest.

13 A Correct. That's correct.

14 Q And you've taken an interest because it's connected with
15 that routing process.

16 A That's correct.

17 Q It may be an innocent user.

18 A Possibly, yes.

19 Q Right. A person might not have -- In fact, very likely
20 that just an ordinary user of *Freenet*, they would have no idea
21 that a file of interest to you had passed through their node
22 or computer.

23 A I don't know if that's likely or not. I'm not sure if a
24 user of *Freenet* knows how much traffic flows through him or
25 what is known or not.

1 Q Well, do they know the content that's flowing through
2 their computer?

3 A They wouldn't specifically know the content, no.

4 Q Pardon me?

5 A They would not specifically know the content.

6 Q Correct. So these would just be users of *Freenet* who
7 have transmissions running through their computers.

8 A Okay.

9 Q You've got your IP address, right?

10 A Yes.

11 Q And you've got an interest in it because they're
12 connected to the routing process of a file of interest to you.

13 A That's correct.

14 Q They may or may not be someone ultimately that you have
15 an interest in.

16 A That's correct.

17 Q Okay. There are thousands of these every day.

18 A I don't know how -- exactly how many there are. It
19 should be in the thousand to two thousand range; IP addresses.

20 Q Okay. Let's say a thousand to two thousand a day, and
21 this operation has been running every day?

22 A Yes.

23 Q Since 2012?

24 A Well, there's two different operations. The one we're
25 talking about now started in 2013; since 2013.

1 Q Okay. But if we go back, we were talking about an
2 operation that began in 2012, too, right?

3 A Yeah.

4 Q If we look at that, we'd say running from 2012 to 2016.
5 It's about the end of -- Well, now we're in 2017. So over
6 five years, right?

7 A Yes, sir.

8 Q Okay. Collecting the IP addresses of all these users,
9 correct?

10 A Correct.

11 Q From the Winter of 2013 on when this newly automated
12 process was put into place, how often -- Let me step back.

13 We've clarified that you got all this raw data at the
14 end of every day, right?

15 Whether it's 2011 or -- Forgive me. Whether it's
16 2012 to 2013 or 2013 on, there's all this data being collected
17 every day, correct?

18 A Correct.

19 Q Okay. And we've established that there are IP addresses
20 and hash values and so on that are included in this database,
21 correct?

22 A Correct.

23 Q Okay. And we've also established that a fair number of
24 these IP addresses are -- at this point you don't know which
25 IP addresses are connected -- are submitters for requests of

1 child pornography. All you know is there are IP addresses
2 involving the routing process of particular files, right?

3 A At this point, yes.

4 Q And so the real trick of the investigation is to figure
5 out who is the submitter; who's the requester of this
6 information.

7 A Correct.

8 Q And that's a bit of a mystery and a technological problem
9 to solve, right?

10 Forgive me. That's not a -- really a question. It's
11 a comment.

12 To solve the problem of identifying the submitter or
13 requester, you need a method to do that, correct?

14 A Correct.

15 Q With all that raw data, you cannot make that
16 determination. All you can see is the raw data, correct?

17 A Correct.

18 Q And this is where the University of Amherst steps in,
19 correct?

20 A They create -- They manage that function for us, yes.

21 Q Right. They created a statistical analysis, right?

22 A Yes.

23 Q An algorithm?

24 A I guess you could call it an algorithm.

25 Q Okay. And that statistical analysis is run through the

1 data that you've collected, correct?

2 A Correct.

3 Q And that statistical analysis gives you some degree of
4 statistical probability ultimately in trying to figure out who
5 is the requester.

6 A Correct.

7 Q How often is that statistical analysis run on the data
8 that's collected?

9 A Daily.

10 Q Daily. So daily there are thousands of IP addresses
11 connected to thousands of files, correct?

12 A Correct.

13 Q And we're uncertain whether or not the individuals to
14 whom these IP addresses are connected are simply routers or
15 requesters, correct?

16 A That's what we need to determine.

17 Q And daily on these thousands of individuals there's a
18 statistical analysis that's run on that data, correct?

19 A Correct.

20 Q And hopefully from the Government's perspective and law
21 enforcement's perspective, that statistical analysis will
22 identify an individual as the likely requester.

23 A Correct.

24 Q And that process has been going on every day since 2012.

25 A The automated process was enhanced in 2015.

1 Q So if we look at the enhanced and the unenhanced version
2 since 2012, that process has been going on every day.

3 A Yes. Somebody -- Somebody had to look at it prior to
4 that --

5 Q Okay.

6 A -- closely to make that determination. It was less
7 automated.

8 Q Now let me make -- So forgive me. This is just for my
9 own edification.

10 The process -- The original process of recording the
11 daily data right now you say is automated. Nobody is looking
12 at that. They come in later and look at it, and then the
13 statistical analysis is run on it.

14 A Yes.

15 Q Okay. And originally the same was true. It was
16 collected overnight. After the fact, somebody would come,
17 look at it, we'll say -- that's poor phrasing really -- and
18 then a statistical analysis would be run on it again, correct?

19 A Correct.

20 Q Okay. So data is copied, stored; a statistical analysis
21 is run on it subsequently.

22 A Correct.

23 Q Maybe every day.

24 A Yes.

25 Q Okay. This is just going back to something we talked

1 about very early on, so forgive me.

2 In each investigation that you had, did you go back
3 and double-check by looking at actual images and files before
4 you go and effect a search warrant?

5 A Yes.

6 Q Okay. The statistical analysis that the University of
7 Amherst developed -- and kudos to them; it's, obviously, quite
8 bright -- is that available to the public?

9 A I don't know the answer.

10 Q Is it for sale anywhere? Do you know?

11 A Not that I'm aware of.

12 Q It might be?

13 A I don't know. I don't think it's for sale, --

14 Q Okay.

15 A -- but I don't know.

16 Q Do you have access to the source code?

17 A I do not.

18 Q And, again, focusing on the statistical analysis that
19 Amherst developed, it is just that, a statistical analysis,
20 correct?

21 A To my knowledge, yes.

22 Q So when the Government was up here questioning you and
23 saying, "This person had that; this person had the other,"
24 really what they mean is within a statistical probability,
25 that information was connected to a specific computer or a

1 specific user; for example, maybe Mr. Dickerman.

2 A Correct.

3 Q And you characterized that as "more likely than not" that
4 statistical probability?

5 A That's what I said, yes.

6 Q Where did you get that piece of information?

7 A "More likely than not"?

8 Q Yeah.

9 A From -- From the developers at Amherst.

10 Q Okay. So you were told that.

11 A That -- Yes.

12 Q I mean you don't know that for a fact.

13 A I don't have the ---

14 MS. LANG: Objection; asked and answered.

15 THE COURT: Sustained.

16 Q (By Mr. Fein) You testified on Direct that *Freenet* is a
17 unique search mechanism, correct?

18 A That it has a unique ---

19 Q No, no; that it is a unique search mechanism. You were
20 testifying that it's unlike other file-sharing programs.

21 A Yeah, in that you don't download from another peer.

22 Q Right. So for example, you've done a lot of work on
23 *Limewire* cases in the past, correct?

24 A Correct.

25 Q Okay. And in *Limewire*, individuals simply download the

1 software, correct?

2 A Yes.

3 Q Okay. And if they -- Whatever files they may have,
4 innocent or otherwise, are stored on their hard drive in their
5 computer, correct?

6 A Yes.

7 Q And you can search the database of *Limewire* users for
8 those files, --

9 A Yes.

10 Q -- correct?

11 A It will index based on the names of those files that
12 you're sharing.

13 Q And you can download them straight from their hard drive.

14 A Right, exactly.

15 Q So you can actually -- And, in fact, they've opened their
16 hard drive to you because, assuming they have *Limewire* set to
17 share, you can reach into the hard drive because they've made
18 it available to all other *Limewire* users and simply download
19 from them.

20 A That's correct.

21 Q They've stored the file on their own computer.

22 A That's correct.

23 Q All right. Whereas with *Freenet*, individuals aren't --
24 the available data to you is not stored on someone's computer
25 in that same way. It's diffused throughout this decentralized

1 network.

2 A Exactly.

3 Q All right. Which is why you can't do the same type of --
4 you can't use the same investigatory technique in *Freenet* that
5 you would use in *Limewire*.

6 A That's correct.

7 Q You helped draft the search warrant for Mr. Dickerman's
8 home?

9 A I provided -- I provided information that may have made
10 it directly to the search warrant. I don't -- I don't think
11 -- I didn't draft the search warrant.

12 Q Yeah. That's poorly phrased, too. Forgive me.

13 The application and the affidavit for the search
14 warrant, ---

15 A I did not draft those.

16 Q Did you review them?

17 A No, I did not.

18 Q Are you aware that you're referenced in them?

19 A I am now. I don't think I was at the time of the search
20 warrant.

21 Q The database we were discussing earlier that contains all
22 the information that's still being collected and the daily
23 runs that are being accomplished, is that all at Amherst or is
24 that something you store?

25 A I don't -- It's not at Amherst. I believe it's at ICAC

1 in Pennsylvania someplace.

2 Q In Pennsylvania somewhere. At ITEC?

3 A ICAC, I-C-A-C.

4 Q Oh, International -- Internet Crimes Against Children.

5 A Yes.

6 Q Can you explain how they function?

7 A I don't know if I can, completely accurate. They're --
8 They're funded through federal grants under the Protect Act,
9 and there's a centralized group that provides training and
10 technical services, and that's -- that's where the database is
11 held.

12 Q That's where the database of images are held?

13 A No. This would be the data.

14 MS. LANG: Objection; speculation.

15 Q (By Mr. Fein) If you know.

16 A I mean that's where the data is that we're collecting
17 that you're talking about; not the images.

18 THE COURT: I'll overrule it.

19 A Not the nodable library.

20 Q (By Mr. Fein) The data that's collected is stored there?

21 A That's my understanding.

22 Q Not the image files.

23 A Not the image files.

24 Q Okay. Forgive me.

25 Earlier -- Just to go back to hash values, and

1 forgive me if I'm repeating myself. I'm sorry.

2 The hash values, as the Government said, are unique
3 identifiers, correct?

4 A Correct.

5 Q So, once again, the hash value of a given file, I see
6 that hash value again; within a very high degree of
7 probability, I know it's the same file.

8 A Absolutely.

9 Q You'll read cases, and they'll call it the equivalent of
10 a technological fingerprint or DNA.

11 A Yes.

12 Q The system you used between the Summer of 2012 and the
13 Fall of 2013, was that peer reviewed?

14 MS. LANG: Objection; relevance, speculation.

15 THE COURT: What -- What is your question?

16 MR. FEIN: I'm curious whether the method, the
17 investigative technique they were using at that time, had been
18 peer reviewed. They were at that time -- Forgive me. Let me
19 step back.

20 At that same time they're using a statistical
21 analysis, an algorithm to make determinations about who likely
22 requesters are. I'm curious if that algorithm, that
23 statistical analysis, was peer reviewed; whether or not it was
24 scientifically sound or not.

25 THE COURT: I'm sorry. Go ahead.

1 MR. FEIN: And he may not know.

2 MS. LANG: But this case and the suppression of
3 evidence that the defense is asking for has to do with a 2015
4 search on *Freenet*.

5 THE COURT: You're asking about the original -- the
6 2012 -- What are you asking about? Which section?

7 MR. FEIN: That's correct, Your Honor. You're right,
8 the 2012 to 2013.

9 THE COURT: Okay. So what relevance does that have
10 to this search?

11 MR. FEIN: Well, I'm not sure yet, but here's what I
12 will say: I don't know what changes were made to that. So as
13 far as I know right now, that's the same statistical analysis
14 that's being used today.

15 THE COURT: Well, you could ask that question,
16 whether there's a change, but I don't -- I don't know that
17 whether the methods that were -- were being used in 2012,
18 whether that was peer reviewed, I don't know what relevance --

19 MR. FEIN: Fair enough. I'll ask it that way.

20 THE COURT: -- that would have to the 2015 search.

21 Q (By Mr. Fein) If you know, again, because you may not,
22 the statistical analysis that's run today and that was in
23 place in 2015, is it the same statistical analysis that was
24 available to you in 2012 and '13?

25 A No, it isn't.

1 Q Okay, very good. Do you know if the one that's in
2 place -- Is the one that's in place now the same one that was
3 in place in 2015?

4 A Essentially, yes.

5 Q What's -- Are there differences? You said "essentially."
6 That's why I asked.

7 A No. It's -- We track additional data or we provide
8 additional numbers, I guess, for -- for an investigator.
9 We'll give them a range of what that percentage is rather than
10 a specific percentage.

11 Q What are the -- What's the additional data that's
12 tracked?

13 A There's no additional data that's tracked. It's the same
14 data.

15 Q Okay.

16 A It's just how the math is, I guess, processed on it.

17 Q So ---

18 A So, no, there really is no difference today than what we
19 were doing in 2015.

20 Q Okay. In 2015 -- In April of 2015 had that been peer
21 reviewed?

22 A It has been peer reviewed.

23 Q No, no. My question is ---

24 A Was it then?

25 Q Yes.

1 A I don't know.

2 Q You don't know.

3 A No.

4 Q Was that your answer?

5 A Yes.

6 Q Okay, fair enough. Did you have -- Did you play any role
7 in the design of the software that did the logging at all or
8 was that all University of Amherst?

9 A After the initial patch, what they did subsequently, it
10 was all University of Amherst.

11 Q Your involvement was limited to 2012 to 2013, the
12 original work.

13 A I worked with Amherst all through this process, --

14 Q Okay.

15 A -- but I didn't design the subsequent version.

16 Q Are you aware of any design problems in the current
17 system you're running?

18 A No.

19 Q Any implementation problems?

20 A No.

21 Q During the -- During the process of the investigative
22 technique, the computers, are there still one to eight
23 computers operating at a given time?

24 A No. Those -- Well, some of those may still be operating.
25 I would suspect there's quite a few more than that right now.

1 Q How many now?

2 A 30; 30ish.

3 Q Okay. And, again, each one collecting thousands of bits
4 of information every day.

5 A Yes.

6 Q Okay. How long has that been going on with 30 of them?

7 A Two years.

8 Q Two years?

9 A Maybe.

10 Q Approximately?

11 A That -- That number fluctuates.

12 Q Okay. And these 30 or so computers running modified
13 *Freenet* are in the *Freenet* system, correct?

14 A Correct.

15 Q So when a datastream comes, they respond in some way,
16 right?

17 I mean *Freenet* -- *Freenet* computers will either send
18 back a block to a computer involved in the routing request or
19 not, right?

20 If it has it, it will return the block; if it
21 doesn't, it will not.

22 A That's correct.

23 Q What message -- What transmission does the law
24 enforcement *Freenet* node send back to the peer that's
25 connected to it?

1 A It -- It will typically send back what any other *Freenet*
2 node would send back. If it has the block, it'll send the
3 block back. If it gets the block from one of its downstream
4 peers, it will send the block back.

5 Q So the law enforcement *Freenet* node might actually send a
6 block of child pornography back to another connected computer?

7 A It could.

8 Q To be routed back to whoever the requester may be?

9 A Yes.

10 Q Okay. And if not, if that block isn't available on the
11 law enforcement modified version of *Freenet*, what will the --
12 what transmission will the computer send?

13 A It will -- If it can't find the block, it would send back
14 a negative response; basically, "I can't find the block."

15 Q Well, was there a point in time when the message -- when
16 the transmission returned by law enforcement *Freenet* was that,
17 "The block cannot be found"?

18 A That option is available if you turn it on in the law
19 enforcement *Freenet* node version.

20 Q Okay. Do you know if that option is on on any of the 30
21 computers running?

22 A I do not.

23 Q So it could be on.

24 A It could be.

25 Q Okay.

1 A It was off by default.

2 Q I got you. But it could be on.

3 A It could be on.

4 Q And when it's on, it sends a message that it cannot be
5 found; that is, the block cannot be found.

6 A Correct.

7 Q It has an effect on the operation of the network itself,
8 how it functions.

9 A It would -- Yes. It will cause the request to be sent to
10 somebody else.

11 Q Right, so keep that going. Okay. So one in three
12 responses. One is "can't be found," right?

13 A Correct.

14 Q One is return the block.

15 A Yes.

16 Q And one is "don't have the block."

17 A It would be the same as "can't be found."

18 Q Okay. Okay. And just to be clear, so if it sends the
19 block back, it's contributing to the requester's aggregation
20 of all the blocks to build the file.

21 COLLEEN LANG: Objection; asked and answered.

22 THE COURT: Sustained.

23 Q (By Mr. Fein) Do you know on a given day how many times
24 a block is sent back from a law enforcement node?

25 A I do not.

1 Q It could be few; it could be many.

2 A Yes.

3 MR. FEIN: I have no further questions.

4 THE COURT: How much Redirect do you have?

5 MS. LANG: Not very much.

6 THE COURT: Okay. I want to take a break.

7 MS. LANG: You want me to go ahead?

8 THE COURT: Yes, go ahead. Yeah, I want to take a
9 break at some point. Yeah, you can go ahead.

10 MS. LANG: Okay.

11 REDIRECT EXAMINATION

12 QUESTIONS BY MS. LANG:

13 Q Investigator Becker, on Cross you were asked about
14 *Limewire* which is a different peer-to-peer network, correct?

15 A Correct.

16 Q And when law enforcement is looking for child pornography
17 offenders on *Limewire*, they are actually connecting and doing
18 a single-source download from a user of *Limewire*.

19 A Yeah. Technically it's the *Gnutella* network. *Limewire*
20 was just one client on that network. But, yes, that's exactly
21 right.

22 Q And that's different from what law enforcement's doing on
23 *Freenet*, correct?

24 A That's correct.

25 Q *Freenet* law enforcement is passively logging

1 communications that are ---

2 MR. FEIN: Objection, Your Honor. So the
3 characterization of "passive" is a characterization -- She can
4 ask the question, but that's a characterization that, I think,
5 is not really established, particularly by the responses
6 Mr. Becker gave about (a) returning blocks and (b) indicating
7 that there may not be any block available in which case
8 requests are routed on through the system. So I understand
9 she may have an interest in saying that, but that word is a
10 modifier. It doesn't need to be there, so I'm going to object
11 to that characterization.

12 THE COURT: I'll overrule it.

13 MS. LANG: Thank you, Your Honor.

14 Q (By Ms. Lang) On Direct Exam, Investigator Becker, you
15 said that the law enforcement node on *Freenet* is passively
16 logging data.

17 A Correct. We don't do anything to suggest we have the
18 data. Our peers will just, as the way the network flows, will
19 send requests to us.

20 Q And the only data that is being stored is data that was
21 sent to you from your peers, correct?

22 A Correct.

23 Q And the only IP addresses that you could ever see on
24 *Freenet* are from your peers or sometimes former peers.

25 A Correct.

1 Q So law enforcement is not indeterminately collecting all
2 types of information from *Freenet*.

3 A No.

4 MR. FEIN: Again, Your Honor, I have to object to
5 that. I mean we've discussed earlier what -- the data they're
6 collecting. So to say that they're not collecting data seems
7 to fly in the face of everything we've discussed.

8 THE COURT: She said "indeterminately," and I heard
9 the previous testimony.

10 MR. FEIN: Fair enough.

11 THE COURT: So I do understand. So you may proceed.
12 I'll overrule the objection.

13 Q (By Ms. Lang) And then going to the statement "more
14 likely or not," that was discussed on Cross. Now based on the
15 statistical algorithm that you're using and we'll talk about
16 Mr. Dickerman's case in particular, when the "Percent of Even
17 Share" is 501 percent that the law enforcement node is getting
18 from its peer, Mr. Dickerman, I mean isn't it true that that's
19 more likely or not that he's the requester of the file?

20 MR. FEIN: I'm going to object. He's already said
21 that. He was told that "more likely or not" is the
22 statistical probability, so that's something he was told. I
23 don't think anything changed from the time of Cross
24 Examination to now that gave him firsthand knowledge of that
25 information.

1 THE COURT: Where are you -- Where are you going with
2 this?

3 MS. LANG: I'm just trying to clarify his answer that
4 on his own as a law enforcement officer, when he's drafting
5 search warrants, he can look at these -- these numbers, these
6 probabilities, and determine whether it's more likely or not.

7 THE COURT: So he's relying -- So you're establishing
8 that he is relying on the statistical analysis provided to
9 make a -- to make a determination or to -- for a search
10 warrant. Is that basically what you're ---

11 MS. LANG: Yes; that he can make his own
12 determination.

13 THE COURT: Based on the analysis that ---

14 MS. LANG: Based on the analysis, correct.

15 THE COURT: Okay.

16 MR. FEIN: It seems to me it would be fair to say he
17 can make a hearsay determination that there's -- that there's
18 more likely than not because that is what he testified to,
19 Your Honor.

20 THE COURT: What is your question again? I'm sorry.
21 I've become lost in the -- in the argument. What was your
22 question?

23 MS. LANG: Well, just even -- In particular, in
24 Mr. Dickerman's case where the "Percent of Even Share" --
25 Investigator Becker can look at that and see that it's 501

1 percent. He's getting five times as much of the request from
2 -- from this peer. So he can look at that and determine that
3 more likely or not, Mr. Dickerman is the actual requester and
4 not a relayer.

5 THE COURT: First of all, I -- if the -- He has
6 already testified to this, and I already -- I have it. I've
7 got it.

8 MS. LANG: Okay.

9 THE COURT: So I mean if -- It's basically asked and
10 answered. I -- I think that between the testimony that he has
11 given on Cross Examination and with regard to the statistical
12 analysis as well as his previous answer is sufficient. So --

13 MS. LANG: Okay.

14 THE COURT: -- I'll sustain the objection.

15 MS. LANG: And could we -- Your Honor, at this point
16 I'd like to put Exhibit 9-A back on the screen momentarily.

17 THE COURT: Okay.

18 Q (By Ms. Lang) And going back to Exhibit 9-A,
19 Investigator Becker, by the nature of peer-to-peer file
20 sharing, isn't it true that communication ---

21 MR. FEIN: Your Honor, I'm sorry. I can't see it.

22 THE COURT: I don't see it either.

23 LEGAL ASSISTANT: Hold on. I'm getting there.

24 THE COURT: Technical difficulties. There we go.

25 Q (By Ms. Lang) Investigator Becker, by the nature of

1 peer-to-peer file sharing, communication on *Freenet* is being
2 made between these peers, correct?

3 A Correct.

4 Q And you have to communicate with a stranger peer on
5 *Freenet* to get what you want.

6 A In Open Net, that's correct.

7 Q Correct. And *Freenet* even warns the user right after the
8 download stage, correct?

9 A Warns? You mean when installing the file?

10 Q Yes.

11 A Yeah. It immediately -- When he's installing the file
12 and setting it up, *Freenet* warns you that what you're doing
13 can be detected.

14 Q So looking at Exhibit 9-A, is that an example of a
15 warning that *Freenet* gives that even though it is -- it says
16 that it tries to be safer than peer-to-peer networks like
17 *BitTorrent*, an attacker with moderate resources may be able to
18 trace your activity on *Freenet* back to you?

19 A That's correct.

20 Q And that's basically what law enforcement's doing,
21 correct?

22 A Correct.

23 Q Using moderate resources, you can trace the IP address
24 back to the original ---

25 MR. FEIN: I object. This "moderate" doesn't really

1 tell me anything.

2 THE COURT: Well, it's -- it's set forth in this
3 warning.

4 MS. LANG: Okay.

5 MR. FEIN: I understand.

6 THE COURT: That's why she's using it.

7 MR. FEIN: Very good.

8 THE COURT: And this is with regard to "Low
9 Security," and we know there's another little page for "High
10 Security."

11 MR. FEIN: Right.

12 THE COURT: So this is -- this is where we are. I'll
13 allow it.

14 Q (By Ms. Lang) And this is what law enforcement's doing
15 on *Freenet* --

16 A Correct.

17 Q -- basically.

18 MS. LANG: I don't have any other questions,
19 Your Honor.

20 THE COURT: Yes.

21 MR. FEIN: Two more questions, Your Honor.

22 THE COURT: Okay.

23 MR. FEIN: Very fast.

24

25

1 RECROSS EXAMINATION

2 QUESTIONS BY MR. FEIN:

3 Q Do you know if Mr. Dickerman ever saw Exhibit 9-A? Do
4 you have firsthand knowledge if he ever saw that?

5 MS. LANG: Objection; speculation.

6 MR. FEIN: I'm asking if he has firsthand knowledge.

7 THE COURT: I'll allow the question.

8 A He had *Freenet* installed on his computer.

9 Q (By Mr. Fein) No. I'm asking you if you have firsthand
10 knowledge that he saw that.

11 A No, I don't.

12 Q I'm not asking you if he had *Freenet*.

13 A I wasn't there when he installed it.

14 MR. FEIN: Very good. Thank you.

15 THE COURT: Okay. All right. Is that all?

16 MS. LANG: Yes, Your Honor.

17 THE COURT: All right. You may step down.

18 We are going to take -- First -- Go ahead and step
19 down now.

20 Do you have -- Who are you calling next? I just want
21 to get an idea.

22 MS. LANG: Detective Slaughter from the St. Louis
23 County Police Department.

24 THE COURT: All right. Well, what we could do -- I'm
25 just trying to figure out. We're getting close to noon, but I

1 want to take a break. So my thought would be: Why don't we
2 just go ahead and take the lunch break early and then we'll
3 start back. So let's -- If it's okay with everyone, can we
4 start back at 12:30?

5 MS. LANG: Yes.

6 THE COURT: That's a little less than an hour for
7 lunch, I'm afraid, but it sounds like we have a lot to cover.

8 MS. LANG: Yes.

9 THE COURT: Okay.

10 MS. LANG: And with out-of-town witnesses, obviously.

11 THE COURT: Right. I want to get everyone on.

12 MS. LANG: Yes.

13 THE COURT: All right. So we are going to take a
14 recess until 12:30.

15 MR. FEIN: Thank you.

16 (Court recessed from 11:40 AM until 12:30 PM.)

17 THE CLERK: All rise. Court is back in session. You
18 may be seated.

19 THE COURT: Ms. Lang, you may call your next witness.

20 MS. LANG: Thank you, Your Honor. Detective
21 Slaughter.

22 (The Witness, DETECTIVE MICHAEL SLAUGHTER, Is
23 Sworn.)

24 THE COURT: You may proceed.

25 MS. LANG: Thank you, Your Honor.

DIRECT EXAMINATION

QUESTIONS BY MS. LANG:

Q Please state your name.

A Michael Slaughter.

Q And what's your occupation?

A I'm a Detective with the St. Louis County Police Department.

Q And how long have you been with the St. Louis County Police Department?

A Approximately 12-and-a-half years.

Q And how long have you been a Detective?

A For seven years.

Q And what unit of the Police Department are you assigned to?

A I'm currently with the Special Investigations Unit, and I'm a Task Force Officer with the FBI's Exploited Children's Unit.

Q And before you were a police officer, did you have any other careers?

A I worked as an automation engineer for about 15 to 18 years.

Q And is that in the computer fields?

A Yes.

Q And what type of education or training do you have -- did you have to be an automation engineer?

1 A I have a two-year and a four-year degree in Electronics.

2 Q And you said that you currently are a Detective with the
3 Special Investigation Unit. Do you ever work on crimes
4 involving exploitation of children?

5 A Yes.

6 Q And how long have you been doing those types of crimes?

7 A For seven years.

8 Q And have you ever drafted a search warrant looking at a
9 home or a property for child pornography?

10 A Yes, ma'am.

11 Q And approximately over the last seven years how many
12 times do you think you've drafted such a search warrant?

13 A Over a hundred search warrants.

14 Q And have you ever drafted search warrants that were
15 involved in cases involving peer-to-peer networks?

16 A Yes, ma'am.

17 Q And are you familiar with the elements of the crimes of
18 possession of child pornography?

19 A Yes, ma'am.

20 Q And what experience or training do you have as a police
21 officer in peer-to-peer networks and child pornography?

22 A I've had training through Internet Crimes Against
23 Children's courses along with a presentation from Special
24 Investigations Becker.

25 Q Okay. And the presentation you had from Investigator

1 Becker, was that on the *Freenet* peer-to-peer network?

2 A Yes, ma'am.

3 Q And was that prior to August of 2015?

4 A Yes, ma'am.

5 Q Now I'm going to move towards this investigation which
6 was in 2015. Did you receive any information or -- How did
7 this investigation begin into Alden Dickerman?

8 A My Sergeant of the Special Investigations Unit handed me
9 the investigation for possession of child porn related to a
10 *Freenet* peer-to-peer software.

11 Q And who was your Sergeant at the time?

12 A Sergeant Adam Kavanaugh.

13 MS. LANG: Your Honor, may I approach the witness
14 with an exhibit?

15 THE COURT: Yes, you may.

16 MS. LANG: 21.

17 Q (By Ms. Lang) Detective Slaughter, does Exhibit 21 look
18 familiar?

19 A Yes, ma'am.

20 Q And what is it?

21 A It's a spreadsheet.

22 MR. FEIN: I'm sorry.

23 THE COURT: Yes.

24 MR. FEIN: I can't see it on our screen.

25 MS. LANG: Oh, I'm sorry.

1 MR. FEIN: Thank you.

2 THE COURT: Okay.

3 Q (By Ms. Lang) Does that look familiar, Detective
4 Sergeant or Detective Slaughter?

5 A Yes, ma'am.

6 Q And was this the spreadsheet that you got from
7 Sergeant Kavanaugh.

8 A Yes, ma'am.

9 Q And based on your information, he had gotten this from
10 Investigator Becker, correct?

11 A Correct.

12 Q And based on your knowledge of *Freenet*, did you then look
13 at this information and draft a search warrant for the IP
14 address?

15 A Yes, ma'am.

16 Q Or I guess I should say a search warrant for the home
17 associated with the IP address.

18 A Correct.

19 Q And do you know what home or business was associated with
20 this IP address? It starts with "172" at the top of Page 1 of
21 Exhibit 21.

22 A I'm sorry. The question?

23 Q Do you know what home or property address was associated
24 with it?

25 A I was able to determine a property, residential address.

1 Q And what was that address?

2 A It's on the subpoena. It's in my report as well or the
3 search warrant.

4 MS. LANG: Your Honor, may I approach?

5 THE COURT: Yes, you may.

6 MS. LANG: I'm going to approach with what's been
7 labeled as Exhibit 22.

8 Q (By Ms. Lang) And does that -- Exhibit 22 which is in
9 your hand right now, does that refresh your memory as to what
10 the address was associated with the IP address that starts
11 "172"?

12 A Yes, ma'am.

13 Q And what was the address?

14 A It's 9524 Corregidor Drive.

15 Q And is that here in St. Louis County or in St. Louis
16 County, Missouri?

17 A Yes, St. Louis County, Eastern District of Missouri.

18 Q Thank you.

19 Now after determining that the address was tied to
20 this IP address that you had this information on, did you do
21 any other checks to determine who was living at that property?

22 A Yes, ma'am. We did a subpoena check of the IP address
23 which came back to that particular address. We did an
24 AmerenUE check which also came back to that address, and we
25 did surveillance as well.

1 Q And at that point did you then draft a search warrant
2 based on your investigation and the information you had
3 received from Investigator Becker?

4 A Yes, ma'am.

5 Q Now in front of you is Exhibit 22. What is Exhibit 22?

6 A It's a search warrant; St. Louis County Search Warrant.

7 Q And is that the search warrant that you drafted in this
8 particular case?

9 A Yes, ma'am.

10 Q And if you take a look at it, is that a fair and accurate
11 representation or is that the actual search warrant that you
12 drafted?

13 A This is the actual search warrant.

14 Q Okay.

15 MS. LANG: At this time, Your Honor, I'd like to
16 admit Exhibit 22, the search warrant.

17 MR. FEIN: Just for clarification, he said it's the
18 search warrant. Are we talking about the search warrant or
19 the affidavit or the application?

20 MS. LANG: Okay. I'll be clear, Your Honor.

21 THE COURT: Yes. I think that that would be helpful.

22 Q (By Ms. Lang) Government's Exhibit 2 contains both the
23 application, the affidavit and the actual search warrant
24 signed by the judge, correct, Detective Slaughter?

25 A Correct.

1 MS. LANG: So at this time I'm asking to move all
2 three pieces as one exhibit.

3 THE COURT: Okay. And that's Exhibit 22, correct?

4 MS. LANG: Correct.

5 THE COURT: Okay.

6 MR. FEIN: No objection.

7 THE COURT: All right. Exhibit 22 will be admitted
8 into evidence.

9 Q (By Ms. Lang) All right. Detective Slaughter, I'm
10 putting on the overhead screen or the screen in front of you
11 Government -- the first page of Government's Exhibit 22. And
12 is this the search warrant that you drafted for the
13 Defendant's address?

14 A Yes, ma'am.

15 Q And what was the date that you presented this to a
16 St. Louis County judge?

17 A The 18th day of August, 2015.

18 Q And did you first present this to a St. Louis County
19 prosecutor?

20 A Yes, ma'am.

21 Q And what date was that?

22 A The same date.

23 Q And what judge did you present it to you?

24 A To Judge Borbonus.

25 Q And he's a -- still currently a judge in St. Louis

1 County?

2 A Yes, ma'am.

3 Q And have you taken any other search warrants to this same
4 judge before?

5 A I have.

6 Q And did those search warrants that you had taken in the
7 past deal with peer-to-peer networks?

8 A Yes, they did.

9 Q Was there any conversation that you had with
10 Judge Borbonus that is not reflected in the search warrant
11 itself?

12 A No, ma'am.

13 Q He didn't ask you any questions that are -- that were in
14 regards to the search warrant like I mean any -- anything --
15 Did he ask, for example, what an "IP address" was?

16 A No, ma'am.

17 Q Did Judge Borbonus appear to be a capable and neutral
18 judge?

19 MR. FEIN: I object. It calls for speculation.

20 THE COURT: Sustained.

21 Q (By Ms. Lang) Did Judge Borbonus ask you any questions
22 or make any comments that made you think he was biased in any
23 way?

24 A No, ma'am.

25 Q Did he make any comments that would make you think that

1 he had a conflict of interest in some way?

2 MR. FEIN: I'm going to object, Your Honor.

3 A No, ma'am.

4 MR. FEIN: Speculation.

5 THE COURT: Overruled.

6 A No, ma'am.

7 Q (By Ms. Lang) Did he make any comments that made you --
8 that he had a conflict of interest?

9 A No, ma'am.

10 Q Did he make any comments that made you -- that made you
11 concerned that he didn't understand the material he was
12 reading?

13 A No, ma'am.

14 MR. FEIN: I'm going to object, Your Honor. Again, I
15 don't know what -- If she wants to be specific about a
16 comment, but that seems to be awfully vague.

17 MS. LANG: The defense raised in one of their motions
18 that the judge who signed the search warrant was incapable of
19 understanding what he was reading. So I'm just trying to
20 determine if that was of evidence to the Detective during the
21 actual signing of the search warrant.

22 THE COURT: Right. I will overrule the objection.

23 MS. LANG: Okay. I believe he already answered.

24 THE WITNESS: Yes.

25 Q (By Ms. Lang) Detective Slaughter, I'm now going to

1 direct your attention to the affidavit in this Exhibit 22, and
2 it's not page numbered, but it's about halfway through in the
3 affidavit section. It starts Paragraph 1. And did you draft
4 that paragraph?

5 A Yes, ma'am.

6 Q And did that -- That basically talks about your
7 experience with peer-to-peer investigations and -- and as a
8 police officer on computer crimes, correct?

9 A Yes, ma'am.

10 Q And then below that is Paragraph 2, and in that
11 paragraph, what is that paragraph talking about?

12 A That the search warrant is submitted for the limited
13 purpose of securing a search warrant and doesn't reflect every
14 fact concerning the case.

15 Q And does it also state that it's based on your knowledge
16 but also the information provided to you by other law
17 enforcement officers? Is that correct?

18 A Correct.

19 Q And then in Paragraph 3, it -- it discusses some of
20 Investigator Becker's certifications and background.

21 A Yes.

22 Q Now I'm going to flip towards the back actually and go to
23 paragraphs -- starting with 12 and then on, and I'm still on
24 the affidavit. And Paragraph 12 is a -- What is it talking
25 about?

1 A Well, this affiant ---

2 Q In Paragraph 12. Go ahead.

3 A "This affiant knows from training and experience that
4 computer users can install publicly-available software that
5 accesses a network known as *Freenet*."

6 Q So then Paragraphs 12 through 20 all talk about how
7 the -- what "*Freenet*" is, correct, and how it works?

8 A Yes, ma'am.

9 Q And just generally, what is "*Freenet*"?

10 A *Freenet* is a peer-to-peer software which uses open source
11 software that allows computers to talk amongst themselves.

12 Q And can you request files on *Freenet*?

13 A Yes, ma'am.

14 Q And can you request files of child -- Based on your
15 knowledge, can you request files of child pornography on
16 *Freenet*?

17 A Yes, ma'am.

18 Q And directing your attention, Detective Slaughter, to
19 Paragraph 21 of that affidavit, it says that, "The streams of
20 requests for blocks of a particular file from an IP address
21 can be evaluated to determine if that IP address is the likely
22 requester of the file."

23 A Yes, ma'am.

24 Q What is that talking about?

25 And this is still in the realm of *Freenet*, correct?

1 A Yes.

2 Q Okay.

3 A It's able to determine that an IP address is requesting
4 certain files over a certain time.

5 Q And is that what law enforcement is doing on *Freenet*?

6 A Yes.

7 Q And then sorry for all this jumping around, but I'm going
8 to go back to Paragraph 6 of the affidavit, and that -- that
9 paragraph is basically -- indicates the -- the observations
10 that Investigator Becker made on *Freenet* in this particular
11 case, correct?

12 A Correct.

13 Q That he was able to observe a certain IP address that
14 starts "172," and that was the IP address that went back to
15 the Defendant's home, correct?

16 A Correct.

17 Q And that IP address, as it states, was routing or
18 requesting the suspected file or suspected child pornography
19 blocks; file blocks.

20 MR. FEIN: Your Honor, I object. This is leading, I
21 believe, Your Honor.

22 THE COURT: Sustained.

23 MS. LANG: I'll rephrase, Your Honor.

24 Q (By Ms. Lang) Now, Detective Slaughter, in that
25 paragraph, what -- I guess -- Was Investigator Becker able to

1 determine that the Defendant was the requester of the child
2 pornography?

3 MR. FEIN: Object, Your Honor. That's leading again.
4 Her answer is in the question.

5 THE COURT: I thought you were asking. It didn't
6 sound like a leading question to me. You said "did," correct?

7 MS. LANG: Right.

8 THE COURT: Right.

9 MS. LANG: I'll rephrase.

10 THE COURT: Okay.

11 MS. LANG: I'll -- I'll lay a little foundation, too.

12 Q (By Ms. Lang) Was -- Investigator Becker was the one who
13 initiated this investigation, correct?

14 A Correct.

15 Q And his information was relayed to you through your
16 Sergeant Kavanaugh, correct?

17 A Correct.

18 Q And he did an investigation on this -- on this particular
19 IP address.

20 MR. FEIN: Again, Your Honor, this is leading.

21 THE COURT: This is leading.

22 MS. LANG: Okay.

23 Q (By Ms. Lang) Did he do an investigation on a particular
24 IP address?

25 A Yes.

1 Q And what was that IP address?

2 A 172.12.235.62.

3 Q And what was he able to determine from that -- from his
4 investigation?

5 A That that particular IP address was using the software
6 *Freenet*.

7 MR. FEIN: Object, Your Honor. I don't think this is
8 foundation for any of this. I have no reason to believe he
9 has personal knowledge of what Mr. Becker did.

10 THE COURT: What -- What are you ---

11 MS. LANG: Well, I'm just trying to get at -- So I'm
12 just trying to get out that the search warrant contained
13 certain evidence -- certain elements of the crime and that
14 there was enough information in the search warrant for the
15 judge to sign it. So I'm just picking -- just kind of noting
16 some of these items in the search warrant.

17 MR. FEIN: Whatever she may be noting, there needs to
18 be a foundation. If he doesn't know what Officer Becker did,
19 then there's no foundation for him to provide these answers.

20 THE COURT: He's the one who signed the affidavit,
21 correct?

22 MR. FEIN: He did, but he's responding now to what
23 Officer Becker did. And unless he can testify, "I know what
24 Officer Becker did," then it would seem to me that these are
25 foundationless responses.

1 MS. LANG: Well, I'm asking what he did in response
2 to what Investigator Becker told him, and it's a limited
3 hearsay question just for the purposes of this hearing.

4 THE COURT: Okay. I will allow your question.

5 MS. LANG: Thank you, Your Honor.

6 Q (By Ms. Lang) I'll move -- Did it -- Based on the
7 information you received from Investigator Becker, how was he
8 able to tell it was this IP address?

9 A This -- This Paragraph 6 is from Officer -- I mean
10 Special Investigator Becker.

11 Q Okay.

12 A And he's telling me while reviewing requests by
13 undercover *Freenet* nodes, he observed the IP address beginning
14 with "172" was routing and requesting suspected child
15 pornography file blocks. By the number and timing of the
16 requests, there was significant data indicating that that IP
17 address was the originator, requester.

18 Q All right. Now moving on to Paragraph 7, which is
19 several -- a couple of paragraphs long, did you put this
20 information into the search warrant?

21 A I did.

22 Q And it's the file, correct, of child pornography?

23 MR. FEIN: I object, Your Honor. She just asked what
24 is it.

25 MS. LANG: Okay.

1 Q (By Ms. Lang) What is -- What is Paragraph 7?

2 A Paragraph 7 indicates that Inspector Becker observed on
3 April 2nd, 2015, between 11:08 PM and 11:10 PM that a computer
4 running *Freenet* software ---

5 MR. FEIN: Your Honor, he's just reading the
6 affidavit. I mean the affidavit is in evidence. I don't
7 understand the point of having him simply read the affidavit
8 to the Court. I think that's objectionable.

9 THE COURT: What -- What are -- What is the --
10 Where -- Where are you going with this other than ---

11 MS. LANG: I'm just trying to show that the file of
12 child pornography was described in the affidavit.

13 MR. FEIN: And it's entered as an exhibit already.

14 THE COURT: Yeah, but I'm not -- I mean we have the
15 information --

16 MS. LANG: Yes.

17 THE COURT: -- and we have the -- we have the
18 affidavit, --

19 MS. LANG: Okay.

20 THE COURT: -- and we've actually gone over in
21 previous testimony what that SHA --

22 MS. LANG: Okay.

23 THE COURT: -- file alphanumeric thing was.

24 MS. LANG: Okay. I'll -- I'll -- I'll ---

25 THE COURT: So I think -- I think I understand that.

1 MS. LANG: I'll get to my point on this.

2 THE COURT: Okay.

3 Q (By Ms. Lang) Did you verify for yourself, Detective
4 Slaughter, that that file was, in fact, child pornography?

5 A Correct. This file actually contained 17 images of child
6 pornography.

7 Q So it was one file that contained 17 images, all of child
8 pornography?

9 A Yes, ma'am.

10 Q Okay. And as -- I know you weren't in the courtroom, but
11 Investigator Becker testified that he actually, on what's
12 Exhibit 21, the spreadsheet, had found that IP address had --
13 multiple times he had -- he had noted that IP address. Why
14 didn't you put in any of the other files?

15 A Yes, ma'am. Under that IP address, two other files were
16 indicated in early June of 2015 that were known child
17 pornography video files. Those files were not put in the
18 search warrant affidavit because they did not fit the scope of
19 the subpoena for the IP address from AT&T.

20 MR. FEIN: This is not relevant, Your Honor. I don't
21 know what the relevance is of files that weren't included in
22 the affidavit.

23 THE COURT: You did ask about them. There was some
24 discussion of those June files in the officer's testimony.

25 MR. FEIN: There was.

1 THE COURT: Yeah.

2 MR. FEIN: There was no Cross Examination about
3 those. So I don't know if we're talking about the affidavit,
4 the search warrant or the application. I simply don't
5 understand the relevance of the additional files.

6 THE COURT: Of why it wasn't included in this one?

7 MS. LANG: I'm just pointing out that the information
8 was supplied to Detective Slaughter but then didn't go any
9 further. I'm just kind of filling in the timeline really.

10 THE COURT: Okay. I'll -- I will allow that since
11 we've had some discussion about the June files, and it is not
12 included in this warrant.

13 Q (By Ms. Lang) On what -- On August 18th, 2015, the
14 search warrant was executed. Is that correct?

15 A Yes, ma'am.

16 Q And where was the address of where it was executed?

17 A 9524 Corregidor Drive.

18 Q Can you spell that --

19 A Yes.

20 Q -- name for us?

21 A It's C-O-R-R-E-G-I-D-O-R Drive; located in St. Louis
22 County, Missouri; Eastern District of Missouri.

23 Q And approximately what time on August 18th of 2015 was it
24 executed?

25 A I believe between 7:00 and 7:30 PM that night.

1 Q And was anyone home at the time?

2 A Yes, ma'am.

3 Q And who was that?

4 A The Defendant, Dickerman.

5 Q And is he here in the courtroom today?

6 A Yes, ma'am.

7 Q And where is he and where is he seated?

8 A Sitting over at the Defendant's table.

9 MS. LANG: Your Honor, may the record reflect that
10 the witness identified the Defendant?

11 A In the blue shirt.

12 THE COURT: Thank you.

13 MS. LANG: Oh, I'm sorry.

14 THE COURT: Now the record will reflect --

15 MS. LANG: Okay.

16 THE COURT: -- he identified the Defendant.

17 MS. LANG: All right.

18 Q (By Ms. Lang) What happened when the search warrant was
19 executed? What was sort of the first step?

20 A The first step is where -- It's St. Louis County's
21 procedure that the Operational TAC Team executes all search
22 warrants. They went in and secured the house. And after the
23 house was secured, then the Special Investigations Unit was
24 allowed to go in.

25 Q And did you go into the home?

1 A I did.

2 Q And who or what did you do when -- or what did you do
3 when you got into the home?

4 A At that time I encountered Mr. Dickerman.

5 Q And what happened at that point?

6 A I contacted him. I identified who I was and asked him to
7 come out to my vehicle, and I talked to him about the
8 situation.

9 Q Was he under arrest at that point?

10 A No, ma'am.

11 Q And I think I asked this already, and I apologize. Was
12 there anyone else in the home?

13 A No one else was in the home.

14 Q And did he voluntarily come out to the car with you?

15 A Yes.

16 Q And what happened next?

17 A We went out to my vehicle. It's an unmarked vehicle. He
18 sat in the passenger seat. I sat in the driver's seat.
19 Another officer, a detective, sat in the back seat.

20 Q And who was that? Do you remember?

21 A It was Detective John Holliday with the Special
22 Investigations Unit.

23 Q Did the Defendant make any statements?

24 A He did.

25 Q Did you -- Before any incriminating -- Before any

1 statements were made, did you read him his *Miranda* rights?

2 A Yes, ma'am. I told him he wasn't under arrest. I asked
3 him if he knew *Miranda*, and I read him his *Miranda* rights from
4 a St. Louis County Warning Waiver Form.

5 Q Okay. And what rights did you read him from the *Miranda*
6 warning form?

7 A Can I read those rights from the paper?

8 Q Just one moment; yes.

9 (Pause)

10 MS. LANG: Your Honor, may I approach?

11 THE COURT: Yes.

12 Q (By Ms. Lang) And I don't have -- And what did I just
13 hand you, Detective Slaughter?

14 A "St. Louis County Police Department Warning and Waiver
15 Form."

16 Q And I marked it as Exhibit 23 just for the limited
17 purposes of this. But from that form, what rights did you
18 read the Defendant?

19 A All right. "You have the right to" -- I'm sorry. "You
20 do not have the right to make any statement at this time and
21 have a right to remain silent. Anything you say can and will
22 be used against you in a court of law. You're entitled to
23 consult an attorney before an interview and to have an
24 attorney present at the time of the interview. If you cannot
25 afford an attorney, one will be appointed for you."

1 Q And you -- And that's the exact form that you read. Not
2 that -- That's not the exact form, but those are the rights
3 that you read to him.

4 A Yes, ma'am.

5 MS. LANG: For the limited purposes of this exhibit,
6 can I submit Government's 23?

7 MR. FEIN: No objection.

8 THE COURT: Government's 23 will be admitted into
9 evidence.

10 Q (By Ms. Lang) Detective Slaughter, did you -- at that
11 point did you begin asking the Defendant questions?

12 A Yes, ma'am.

13 Q And basically what did he tell you? Just sort of a
14 summary.

15 A That he was the occupant of the house; that he lived at
16 the house. He had several computers at the house, and he
17 indicated which computers he used and didn't use. He also
18 indicated that he had the *Freenet* software on his computer.

19 Q And did he indicate what room of the home was his bedroom
20 with his computers?

21 A He did.

22 Q Did you begin to ask him about child or -- excuse me --
23 pornography on *Freenet*?

24 A I did.

25 Q What happened when you asked him about that?

1 A At that time he requested to have a lawyer present.

2 Q Did you cease all incriminating questions at that point?

3 A Yes.

4 Q Was there any statements made after he asked for a
5 lawyer?

6 A No statements. We talked about the procedure of the
7 process that was -- would happen.

8 MS. LANG: I don't have any further questions,
9 Your Honor.

10 THE COURT: All right. You may cross-examine.

11 MR. FEIN: There's one more.

12 MS. LANG: I believe I have one question to clarify.

13 THE COURT: All right. Go ahead.

14 Q (By Ms. Lang) Can you -- Detective Slaughter, what did
15 -- Can you re-read the beginning of the *Miranda* rights that
16 you read to the Defendant?

17 A Sentence 1?

18 Q Yes.

19 A "You do not have to make a statement at this time and
20 have a right to remain silent."

21 MS. LANG: Thank you. Nothing further.

22 THE COURT: Okay.

23 CROSS EXAMINATION

24 QUESTIONS BY MR. FEIN:

25 Q Good afternoon, Detective.

1 A Good afternoon.

2 Q Just to clarify some confusion in my mind from earlier on
3 during your Direct, initially you were talking about the
4 search warrant but actually referring to all three documents,
5 I believe?

6 A That's correct.

7 Q You indicated that you drafted the search warrant. Do
8 you mean you wrote the search warrant itself?

9 A Correct.

10 Q So you wrote the search warrant, correct? "Yes"?

11 A Yes.

12 Q You wrote the application?

13 A Yes.

14 Q And you also wrote the affidavit.

15 A Correct.

16 Q Okay. I'll direct you to Government's Exhibit 22, and
17 I'm not sure of the order. I'm hoping that the top document
18 is the search warrant itself.

19 A Yes.

20 Q Good. You indicated earlier it's file stamped August
21 18th, 2015; correct?

22 A It is.

23 Q And at the very top there is a division number; Division
24 35?

25 A Correct.

1 Q Did you write that in or did somebody else write that in?

2 A Either I wrote it in or the judge wrote it in.

3 Q Okay. So that would be you don't know?

4 A I don't know.

5 Q Okay. Do you recognize that writing? Does it look like
6 your handwriting?

7 A At times.

8 Q At times that looks like your handwriting?

9 A Yes.

10 Q How about this time?

11 A I can't recall.

12 MS. LANG: Objection; asked and answered. He said he
13 didn't remember.

14 THE COURT: Sustained.

15 Q (By Mr. Fein) At the first full paragraph it has a
16 handwritten date of "18." Did you write that in?

17 A I can't recall.

18 Q Okay. On that same line there's a handwritten name. Did
19 you write that name?

20 A I did not write that name.

21 Q You did not write that name.

22 A No.

23 Q Okay. And in the next line down there's a division
24 number again. Did you write that division number?

25 A I don't recall.

1 Q Forgive me?

2 A I don't recall.

3 Q Okay. The warrant itself is not signed by you, correct?

4 Does not bear your signature.

5 A The search warrant part does not.

6 Q Correct. I'm hoping that the second document is the
7 application for the search warrant. Is that correct?

8 A Correct.

9 Q And if you turn to the second page, that does bear your
10 signature?

11 A It does.

12 Q And that would leave the last document as the affidavit.
13 And if you turn to the next to last page of that or the last
14 page, it bears your signature as well?

15 A Yes.

16 Q Is that your -- Underneath the signature on the last page
17 of the affidavit, there's what I assume is a DSN number?

18 A Correct.

19 Q What is that number?

20 A 3562.

21 Q This is a minor matter. Will you turn back to the
22 application? I just couldn't make it out. That's the same
23 number, "3562"?

24 A It is.

25 Q My writing is atrocious, so I'm not going to criticize

1 yours.

2 You said you met with the judge to ask for a
3 signature on the warrant, correct?

4 A Yes.

5 Q And you indicated that the judge asked you no questions,
6 correct? That was your testimony on Direct.

7 A No, that's not correct.

8 Q Forgive me?

9 A Anything outside the search warrant?

10 Q Correct.

11 A Correct.

12 Q No. I mean he did not ask you to expand on the search
13 warrant, correct?

14 A Correct.

15 Q Let me rephrase that. He did not ask you to expand on
16 the affidavit or the application filed in support of the
17 search warrant, correct?

18 A Correct.

19 Q And you were asked by the Government if you had met with
20 Judge Borbonus previously to ask him to sign warrants, and you
21 indicated you had, correct?

22 A Correct.

23 Q And you indicated that you had done so on peer-to-peer
24 investigations, correct?

25 A Correct.

1 Q Have you ever done so on a *Freenet* investigation?

2 A Yes.

3 Q In which case?

4 A I don't know the case offhand.

5 Q Well, when?

6 A Before August 15th --

7 Q How far before August 15th?

8 A -- of 2015? I don't know.

9 Q Will you get for me that information in that case?

10 A Sure.

11 Q Okay. Well, here's the thing: You're testifying under
12 oath today. You're testifying under oath today that you met
13 with Judge Borbonus for prior *Freenet* investigations to sign
14 off.

15 A No, not *Freenet*.

16 Q Okay. So I had asked you a moment ago about *Freenet*.
17 You said "yes." So now you're saying you've never met with
18 him about a *Freenet* case before.

19 MS. LANG: Objection; compound question.

20 MR. FEIN: I'll state it as a single question.

21 THE COURT: Okay.

22 Q (By Mr. Fein) You've never met with Judge Borbonus
23 before to sign off on a *Freenet* warrant, correct?

24 A I'm sorry. Restate the question.

25 Q Sure. You've never met with Judge Borbonus before to

1 sign off on a *Freenet* warrant, correct?

2 A I cannot say I've never met with him.

3 Q On a *Freenet* case?

4 A On a *Freenet* case.

5 Q Can you think of one right now?

6 A I cannot.

7 Q So the best of your recollection right now, you've never
8 asked him to sign off on a *Freenet* warrant before.

9 A No, I can't recall.

10 Q Okay. So the best of your recollection right now, the
11 answer would be "no," correct?

12 A Okay.

13 Q Not "okay." Correct?

14 A Yes, "no."

15 Q How many users worldwide have *Freenet*?

16 A I'm sorry. Reask the question.

17 Q How many users worldwide have *Freenet*?

18 If you don't know, it's okay to say you don't know.

19 A I don't know.

20 Q How many users nationally have *Freenet*?

21 A I don't know.

22 Q How many files are stored on *Freenet* worldwide?

23 A I don't know.

24 Q How many people daily share files on *Freenet*?

25 A I don't know.

1 Q Would you take a look at Paragraph 17 of the affidavit
2 filed in support of the search warrant?

3 I'll direct you to the last sentence in that
4 paragraph. So that sentence says, "*Freenet* is not a
5 significant source of music, adult pornography, theatrical
6 movies or other copyrighted material." But based on your
7 answers a moment ago, you would have no reason whatsoever to
8 draw that conclusion, correct?

9 MS. LANG: Objection; argumentative.

10 THE COURT: Overruled.

11 Q (By Mr. Fein) You said you have no idea how many people
12 have *Freenet* worldwide or nationally or how many files there
13 are or how many are shared. How would you draw such a
14 conclusion?

15 A Based from my experience that *Freenet* is not typically
16 used --

17 Q Well, let me stop you there.

18 A -- for a source of music, adult pornography, --

19 Q Does it say, "Based on my" ---

20 A -- movies and/or copyrighted material.

21 Q Forgive me. I'm sorry.

22 It doesn't say "based on my experience" in your
23 affidavit, does it?

24 MS. LANG: Objection again.

25 A It says that at the beginning of the paragraph.

1 Q (By Mr. Fein) The sentence that we're focusing on, does
2 it say, "Based on my experience, *Freenet* is not" ---

3 MS. LANG: Objection; argumentative.

4 THE COURT: Sustained.

5 Q (By Mr. Fein) I think I've asked enough about that.

6 Can you show me where in your affidavit it says,
7 "Based on the statistical analysis, we've identified an IP
8 address as a potential requester of child pornography on
9 *Freenet*"?

10 A Excuse me, sir. Ask the question again.

11 Q Can you direct me to the portion of your affidavit that
12 reflects that the statistical analysis of *Freenet* data
13 collected by the Government is what led you to Mr. Dickerman?

14 Where is there a reference about the statistical
15 analysis that was used to identify a probability that
16 Mr. Dickerman was, in fact, a suspect in the case or the
17 target of the search warrant?

18 A There's no such paragraph.

19 Q In fact, there's no reference to a statistical analysis
20 anywhere in the affidavit, right?

21 MS. LANG: Objection; asked and answered.

22 THE COURT: Sustained.

23 Q (By Mr. Fein) I'm going to direct you to Paragraph 6.
24 The last sentence says, "The number and timing of the requests
25 was significant enough." What does "significant enough" mean?

1 A Enough to make me believe that that was the requester.

2 Q And what would you base that on?

3 A In this particular case, the number of peers that were
4 connected to our undercover node.

5 Q What was the probability -- Without referring to another
6 document, what was the probability of that? The statistical
7 probability. Do you know?

8 A I don't.

9 Q Very good. That statistical probability is not reflected
10 in this affidavit either, is it?

11 A I don't include all facts in my search warrants.

12 Q That's not what I asked, Detective. I asked you if the
13 statistical probability was included in the affidavit.

14 A Correct; it's not.

15 MS. LANG: Objection; asked and answered, Your Honor.

16 THE COURT: He's answered it now. Overruled.

17 Q (By Mr. Fein) Let's take a look at Paragraph No. 7.

18 It's says, "Sixty-nine parts or blocks of the following file
19 were requested from *Freenet*;" correct?

20 A Correct.

21 Q It does not say how many blocks in total that file is
22 comprised of, does it?

23 A It does not.

24 Q It doesn't say the percentage of the total that those
25 blocks comprise, does it?

1 A It does not.

2 Q And that's the only file that's listed in the affidavit,
3 correct?

4 A Correct.

5 Q Let's look at Paragraph 21 very quickly, and that would
6 be on the last page -- forgive me -- of your affidavit. Tell
7 me when you're there.

8 A I'm there.

9 Q Oh, thank you. It says, "This Affiant knows from
10 training and experience that streams of requests for blocks of
11 particular files -- of a particular file from an IP address
12 can be evaluated to determine if the IP address is the likely
13 requester of the file." How are they evaluated for that
14 purpose?

15 A We'd have to go to Exhibit 21.

16 Q I'm sorry?

17 A We'd have to go to Exhibit 21.

18 Q What's Exhibit 21?

19 A Your *Freenet* file summary spreadsheet.

20 Q Okay. So I'm just asking you in your words: How are
21 they evaluated for that purpose? What is the evaluation
22 process? If you don't know, that's okay. If you do know,
23 that's okay, too.

24 A Without going to the exhibit, I'm going to say: I don't
25 -- I cannot tell you.

1 MR. FEIN: I have no further questions, Your Honor.

2 Thank you.

3 THE COURT: Redirect?

4 MS. LANG: Thank you, Your Honor.

5 REDIRECT EXAMINATION

6 QUESTIONS BY MS. LANG:

7 Q Detective Slaughter, going to Exhibit 21 that's in front
8 of you, and I'll put it up on the screen, did you have this
9 information when you drafted the search warrant in this case?

10 A I did.

11 Q And were you able to look at this information?

12 A I was.

13 Q And I'm going to direct you to one particular box. It
14 says "Percentage of Even Share." Do you see that?

15 A Yes.

16 Q And what was in this case the "Percentage of Even Share"
17 of requests through the law enforcement node from this IP?

18 A Five hundred and one percent.

19 Q And what does that tell you?

20 A It tells me that the requester was the -- that this IP
21 address was the main requester.

22 MR. FEIN: Forgive me. I missed it. Was the what?

23 THE COURT: "Main requester," I believe, is what he
24 said.

25 Q (By Ms. Lang) And you had this information when you

1 drafted this search warrant, correct?

2 A I did.

3 Q And you also were able to consult with Investigator
4 Becker and Sergeant Kavanaugh when you drafted this search
5 warrant, correct?

6 A I did.

7 Q And the search warrant, as you've said in Paragraph 2 of
8 the affidavit, was it based on your knowledge alone?

9 A No.

10 Q It was also based -- Whose -- Who else's knowledge was it
11 also based on?

12 A Special Investigator Becker.

13 Q And he relayed to you a lot of the information in the
14 search warrant.

15 A Yes.

16 Q Including -- Did he relay you the information that's in
17 Exhibit 21?

18 A He did.

19 MR. FEIN: Forgive me. I missed that. What was
20 that?

21 MS. LANG: I asked if Investigator Becker relayed him
22 the information in Exhibit 21.

23 MR. FEIN: Thank you.

24 Q (By Ms. Lang) Now just to clarify, the words
25 "statistical", "algorithm", are they in the search warrant

1 themselves? The affidavit. Do you remember?

2 A I don't remember.

3 Q Okay. But moving to Paragraph 16 of your affidavit,
4 what's the -- Could -- Could you read the second sentence of
5 Paragraph 6?

6 A 6 or 16?

7 THE COURT: 6 or 16?

8 MS. LANG: 6. I'm sorry; 6.

9 A "The number and timing of the requests has a significant
10 value" -- I'm sorry. "The number and timing of the requests
11 was significant enough to indicate that the IP address was the
12 apparent original requester of the file."

13 Q (By Ms. Lang) That information, number and timing of the
14 requests, where did you get that from?

15 A From Exhibit 21, the spreadsheet.

16 Q Okay. So Exhibit 21 lists the number and timing of the
17 requests. And based on information you received, you wrote it
18 was significant enough to -- What does "significant enough"
19 mean to you?

20 A Okay. Based on the number of requests from that
21 requester, the number of the requests that the undercover
22 *Freenet* node received, was enough to indicate that they --
23 that this computer of "172" was the requester.

24 Q Okay. And so a lot of it ---

25 MS. LANG: Actually I don't have any further

1 questions, Your Honor. Thank you.

2 THE COURT: Mr. Fein?

3 RECROSS EXAMINATION

4 QUESTIONS BY MR. FEIN:

5 Q On Paragraph 6, the number and timing is not listed,
6 correct?

7 It just says the number and timing was significant
8 enough, right?

9 A Correct.

10 Q Significant enough to you, correct?

11 A Correct.

12 Q Based on what Officer Becker told you, correct?

13 A Along with the spreadsheet, correct.

14 Q What does "Percent of Even Share" mean?

15 A I don't know.

16 Q I didn't think so.

17 MR. FEIN: No further questions.

18 THE COURT: All right. You may step down.

19 THE WITNESS: May I leave?

20 THE COURT: You may step down. Yes, I think.

21 And you may call your next witness.

22 MS. LANG: Dr. Brian Levine.

23 MR. FEIN: Your Honor, can I ask Ms. Lang something?

24 THE COURT: Sure.

25 (Pause)

1 MR. FEIN: Your Honor, could we -- There's a witness
2 I need to contact. Can we take about a five-minute break?

3 THE COURT: Sure.

4 MR. FEIN: Forgive me. I've just spoke with
5 Ms. Lang. She thinks her witness will take 45 minutes to
6 Direct, and I suspect I'll have five or ten minutes' worth of
7 Cross Examination.

8 THE COURT: Okay.

9 MR. FEIN: And then she'll be finished, I think, with
10 her witnesses.

11 THE COURT: Okay.

12 MR. FEIN: And I may have one to two witnesses to
13 call, but I would call this witness first. So if I could call
14 or contact him because he is not here.

15 THE COURT: Sure; sure. Okay, yes. Let's take a --
16 Let's take ten minutes. Okay?

17 MR. FEIN: How long?

18 THE COURT: Ten.

19 MR. FEIN: Okay.

20 THE COURT: I'll tell you what: More like seven.
21 It's 1:23. We'll come back around 1:30. Ten minutes? Ten
22 minutes, fine.

23 MR. FEIN: Thanks, Your Honor.

24 THE COURT: We're in recess.

25 (Court recessed from 1:23 PM until 1:35 PM.)

1 THE CLERK: All rise. Court is back in session. You
2 may be seated.

3 THE COURT: You may call your next witness.

4 MS. LANG: Thank you, Your Honor. At this time the
5 Government calls Dr. Brian Levine.

6 (The Witness, DR. BRIAN LEVINE, Is Sworn.)

7 THE COURT: You may proceed.

8 MS. LANG: Thank you, Your Honor.

9 DIRECT EXAMINATION

10 QUESTIONS BY MS. LANG:

11 Q Please state your name.

12 A My name is Brian Levine.

13 Q And what's your occupation?

14 A I'm a Professor at the University of Massachusetts -
15 Amherst in the College of Information and Computer Sciences.

16 I'm also the Director of the Cyber Security Institute there.

17 Q And as a Professor at the University of Amherst, what do
18 you currently teach?

19 A Currently I teach a class on secured distributed systems.
20 *Freenet* is an example of a secured distributed system. In the
21 past I have taught courses on computer networking, data
22 structures, mobile systems, computer and network security,
23 various seminars, but those are the -- those are the main
24 classes.

25 Q And how long have you been in that position at the

1 university?

2 A I joined in 1999 after getting my Doctorate from the
3 University of California - Santa Cruz in Computer Engineering.
4 I joined as a -- what's called a "Tenured Track Professor," so
5 I'm ending my eighteenth year there.

6 Q And you said you have your Doctorate. What other
7 educational background do you have?

8 A I received a Bachelor's of Science in Applied Math and
9 Computer Science from the University of New York at Albany.
10 And then I received, on the way towards my Ph.D., a Masters in
11 Computer Engineering from the University of California -
12 Santa Cruz as well.

13 Q And do you have any training or experience in
14 peer-to-peer networks?

15 A Yes, a great deal. Peer-to-peer networking was actually
16 the follow-on topic for my dissertation in grad school. It's
17 something I've been investigating as a researcher since
18 probably 2000, maybe 2001; I can't recall. But I've had
19 various research grants from the U.S. Government, including
20 the National Science Foundation on peer-to-peer networking.

21 Peer-to-peer networking is a broad topic that covers
22 not only mobile phones or mobile devices but also file-sharing
23 networks like we've seen here in *Freenet* as well as more
24 common examples like *BitTorrent* and *Gnutella* and other --
25 other file-sharing peer-to-peer networks.

1 Q And do you have any -- Have you done any specific
2 publications on peer-to-peer networks?

3 A Yeah, quite a number, and those publications are on a
4 variety of topics that range from characterizing how these
5 peer-to-peer networks are used and practiced. I've researched
6 anonymous protocols, such as *Tor* which is something that's
7 like *Freenet*. I've done work on *Bitcoin* which turns out to be
8 at its core a peer-to-peer network, and I've looked at many
9 mobile systems. And so -- In fact, I've had publications that
10 illuminate vulnerabilities in *Tor*, and those vulnerabilities
11 have been reacted on by the *Tor* developers to change what
12 they're doing to be more secure.

13 I've noted vulnerabilities in a peer-to-peer
14 file-sharing network called "*OneSwarm*" which is -- shares a
15 lot of common features with *Freenet*, and those developers
16 modified what they were doing based on my findings of
17 vulnerabilities.

18 I've also proposed protocols that allow for privacy
19 in various contexts. So, for example, I have a proposal for
20 increasing the privacy of people who use *Bitcoin*, proposals
21 for adding privacy to users of cellular phones. And like I
22 said, really the papers that we publish on things like *Tor* are
23 used by developers to increase the privacy once they're aware
24 of the vulnerabilities that we're -- that we've published and
25 has peer-reviewed papers.

1 Q And you talk about *Tor*. Have you ever testified in
2 federal court before?

3 A I have testified in federal court once before.

4 Q And was that on -- about a peer-to-peer network, also?

5 A It was about -- It was about *Tor* generally.

6 Q And isn't it true that you're paid to be an expert
7 witness for the Government today or you're paid for your
8 services?

9 A I'm paid today to be here as well as travel expenses.

10 Q Thank you.

11 Now I'm going to direct my attention more to *Freenet*
12 as a peer-to-peer network. Do you have any experience with
13 *Freenet*?

14 A I do have experience with *Freenet*. For example, we have
15 a recent peer-reviewed paper on -- on techniques for -- for
16 distinguishing between relayers as we've been talking about
17 today, relayers of requests and actual requesters of files in
18 *Freenet*.

19 Q And you said that paper is currently being peer reviewed
20 or has already been?

21 A Well, the peer-reviewing process for the paper is
22 complete which is to say we submitted the paper. Reviews have
23 come back from a selection of experts that are involved in
24 that process. The final stage is to go to a small event and
25 to present the paper, and that has not happened yet, but

1 the -- So in that sense, the paper wasn't officially published
2 at that event, but the peer-review process is over.

3 Q And who peer reviewed this publication that you have on
4 *Freenet*?

5 A It appears in the IEEE International Workshop on Privacy
6 Engineering, which takes place in -- I forget the exact date
7 but it's May of this year, May of 2017, and IEEE -- Well, let
8 me say a few things, if you don't mind.

9 IEEE is the -- one of the two major professional
10 societies for computer scientists and electrical engineers.
11 They perform a lot of activities but are very commonly a
12 sponsor of -- of reputable workshops and conferences. This is
13 a workshop that's attached to the main IEEE conference on
14 computer security.

15 I'm sorry. Did I answer your full question?

16 Q Well, I -- I asked who -- who are the peer reviewers?

17 A Okay. I'm sorry. So in order to submit papers to this
18 workshop, they ahead of time gather together a collection of
19 academics and experts, possibly professionals. I don't know
20 for this exact workshop whether it's distinctly professionals
21 or only academics, but it's publicly available, this
22 information. My recollection is it's something like 20
23 different experts who research in this case privacy and
24 privacy engineering specifically for, for example, networking
25 topics likes *Freenet*.

1 And then this is a double-blind conference which
2 means that -- Well, so the -- These reviewers are put
3 together, and then we submit the paper. We leave our names
4 off the paper. That's the first part of the blind review.
5 And then the reviewers don't know our names, and they submit
6 their review back to us. I also don't know who reviewed the
7 paper. I only know it was among the collection of people
8 who -- the collection of experts who were gathered together to
9 do the reviews.

10 Once the paper was accepted, I believe all papers in
11 the workshop, although I'm speculating, but our paper, in
12 particular, I know for sure went through what's called a
13 "shepherding process." And what that means is we were given
14 the reviews and then we responded to the reviews. We
15 addressed the reviewers' concerns. We -- You know, they had
16 lingering questions, and we said, "Well, here's the answer to
17 this; here's the answer to that."

18 The shepherd is someone from the Program Committee,
19 the collection of experts; quite possibly the one who reviewed
20 the paper; I don't know. And they ensured that we stuck to
21 what the reviewers want us to clarify, and then we submitted a
22 new version of the paper that will be -- that -- that
23 addressed those concerns and so on. So it's pretty -- pretty
24 heavily reviewed for a workshop paper as it goes.

25 Q Now in your career experience, have you ever worked in

1 the field of cases involving child exploitation?

2 A Yes. I should say that as part of my work on
3 peer-to-peer networking, we -- we quickly learned that -- I
4 mean quickly, I mean back in 2000s; early 2000s. We quickly
5 realized that file sharing on peer-to-peer networks were very
6 actively used by people who were trading child exploitation
7 materials.

8 Also, at the time I had an increased interest in
9 digital forensics, including what I would call "network
10 forensics" which is simply the application of
11 forensically-sound techniques to network investigations as
12 opposed to simply looking at a local computer. So it occurred
13 to me that that's an important issue, and we'd like to learn
14 more and research more and develop novel techniques, strong
15 techniques for investigating crimes that take place on
16 peer-to-peer file-sharing networks.

17 So I've written papers that are available publicly
18 now that talk about how to do -- that are peer-reviewed
19 papers, how to do forensically-sound investigations on things
20 like *BitTorrent*, on *Gnutella*, on *OneSwarm*. I may be
21 forgetting a few, but those are examples. And certainly, as I
22 explained here, the most recent paper is on how to do a
23 forensically-sound investigation from my scientific point of
24 view on *Freenet*.

25 Q How does -- Can you briefly describe what "*Freenet*" is

1 and how it works?

2 A So *Freenet* -- To repeat some of what's been said today,
3 I'd like to refresh everyone a little bit and to put it in my
4 own words. *Freenet* is a peer-to-peer network that enables
5 file sharing by a collection of peers. We mean a series of
6 users who have a computer at home and probably a pretty good
7 Internet connection as it's commonly available these days, and
8 they are lending their resources to other peers in the
9 network. So that in the example of -- In the case of *Freenet*,
10 files can be stored in the network, and they're, as we've
11 heard, literally broken up into pieces and stored on all the
12 other peers' computers. And, of course, some of other users'
13 inserted files are stored on any particular users. But in
14 exchange, they're able to query these files or retrieve those
15 files that had been previously stored.

16 So -- So what's special about *Freenet* is that not
17 only does it provide this storage and retrieval of files but,
18 in particular, it allows for the anonymous insertion, what
19 we'll call the "anonymous insertion" which I'll define in a
20 minute and also the anonymous retrieval of those files. And
21 as a few people have said today, the fact that you're using
22 *Freenet*, your IP address is distinctly available to your
23 direct peers on the network. I mean when you join, you --
24 there's a process by which you receive essentially randomly a
25 set of neighbors on the network. Those are your peers, and --

1 and they certainly know that you're using *Freenet*. But the
2 fact -- The distinction between whether you're relaying a
3 request for a file from someone or whether you yourself are
4 the requester of that file, that's -- that's *Freenet*'s mangle
5 is to make those two roles indistinguishable.

6 Q When was *Freenet* created and how?

7 A My recollection is that it was created from an academic
8 paper back in -- I believe it was 2001. If not, certainly
9 around that year. As I said, I was already -- I had already
10 started as a Professor, and peer-to-peer networking was a
11 strong interest of mine. So I don't remember the precise day
12 or year in which I first learned about *Freenet*, but I -- I do
13 recall that publication.

14 Q And *Freenet* uses a decentralized database. What does
15 that mean?

16 A I prefer to use the word "data store" but "database"
17 isn't terrible. This relates to what I said before. When
18 files are inserted into *Freenet*, you are collectively, as a
19 user who has inserted that file, you're using the collective
20 resources of all the peers who have volunteered to dedicate
21 some of their local computer's hard drive to your -- to the
22 file that you would like to insert. And there's a complicated
23 process from there as to whether that -- that file will
24 survive and how you request it, but the idea of the data store
25 is that you're storing some pieces of many different files

1 inserted by your fellow peers or even peers you're not
2 directly connected to on the *Freenet*.

3 Q Is that the only way files are stored on the *Freenet*
4 network? In the -- In the individual node data stores?

5 A Yes.

6 Q There's not like one -- Is there one large server
7 somewhere hosting files?

8 A No. If you would compare it to -- For example, I have a
9 subscription to *Spotify*. *Spotify* is distinctly not a
10 peer-to-peer service in that sense. They are a central
11 provider. They are a centralized database. There are some
12 tricks there about whether -- how they do that, but, you know,
13 in comparison to *Freenet*, to elate some details, there's no
14 service provider who's making money off this. It's peer to
15 peer in the sense that there's just a bunch of users who
16 volunteered their computer in hopes of, again, retrieving the
17 files of others or perhaps inserting some files of their own.

18 Q And after files are inserted into *Freenet*, how can
19 someone request a file from the system?

20 A So as was explained earlier today, *Freenet* provides an
21 interface mostly commonly through, as we saw, through --
22 through a web browser, and there's a series of, say, index
23 sites or free sites. There's the *Frost* messaging board.
24 Users will post a key, for example, and that key can be copied
25 and pasted into the browser, say, you know. The exhibits

1 earlier today are really what I'm referring to. Those were
2 correct in the sense of any user can -- can easily -- I mean
3 anyone can run *Freenet*. As we saw, the software is free.
4 Anyone can in its use discover keys to these files and then
5 retrieve it using the *Freenet* software. There's -- There's no
6 special requirement.

7 Q You said the -- How are the -- You said the files are
8 divided into different -- into blocks stored on different
9 peers. So when they're -- And you talked earlier about a
10 requester and a relayer. When they're recovered, how does the
11 -- how does the -- how do you know who's the requester versus
12 the relayer of -- of who's asking for the file blocks?

13 A How might one distinguish those two roles?

14 Q Yes. Thank you.

15 A Do you mind if I might go into some detail?

16 Q No. Go ahead.

17 A Okay. Do you mind if I do this by analogy?

18 Q No.

19 A Okay. So let's assume that there's a file that's already
20 been inserted into *Freenet*, and so let's assume that it's
21 already been disbursed around the network, and that process is
22 roughly random. One large file might be split into a thousand
23 pieces that are distributed among many of the peers that exist
24 in the network.

25 Now your job as a requester is to retrieve those

1 pieces. And the game, so to speak, that *Freenet* is playing to
2 make it hard to distinguish the roles of requester and relayer
3 might be suitable by this analogy.

4 So let's say that we have a classroom, and someone's
5 got a bag of, let's say, 100 M&Ms, and we want to distribute
6 these M&Ms. And so the person who's holding the bag of M&Ms
7 is going to give an even share to their friends. They're not
8 going to give them one by one to each person in the class. In
9 *Freenet* it works differently. It's perhaps a -- Well -- So
10 the person holding the M&Ms might give it to four of their
11 friends in the class, and some of them will get 25; some of
12 them might get 20; some of them might get 30. Now the goal is
13 to distribute the M&Ms to the class using this process. So
14 those intermediaries will, in turn, turn to four of their
15 friends and distribute those M&Ms. And they only have, say,
16 about 25 to distribute.

17 So the question is not an estimation of how many M&Ms
18 should I get. It's by looking at the M&Ms that I received, am
19 I -- did I receive these M&Ms from someone holding the bag?
20 And we would know that by looking at how many we got. We
21 might get 20. We expect somewhere between -- around 25 or did
22 I get these M&Ms from someone who themselves got them from the
23 holder of the bag?

24 Now the important thing here is that this isn't --
25 this -- this -- this question I'm posing is not an estimation

1 of the number of M&Ms I have. I'm asking whether I'm next to
2 the person holding the bag or not.

3 Similarly -- I mean that's a very distinct type of
4 question that's easier to answer. For example, in that class,
5 if someone asks me what grade am I going to get, I might say,
6 "I don't know; an A or an A-." But if they ask me, "Are you
7 going to pass," I can say, "Yeah, I'm going to pass this
8 class." That's an easy question to answer, but an estimation
9 of my grade is a much more harder thing to do.

10 So -- So, again, this process, I'm really asking:
11 Are you -- Are you next to someone who's holding the bag of
12 M&Ms or are you getting your M&Ms, given that you know they're
13 divided about equally each time, you know, getting it from
14 someone who is, in fact, not -- not holding the bag.

15 Now because -- That's just an analogy, right?

16 And in reality, sticking with our example a little
17 bit, someone might get a little bit more from the person
18 holding the bag and someone might get a little bit less. Oh,
19 I'll give a little bit more here to this person because I know
20 they have four more friends to distribute to. But it doesn't
21 -- To answer the questions of whether you're next to someone
22 holding the bag is, again, a much easier question.

23 And so if we talk about the way *Freenet* really works,
24 there's a lot of intricacies to how it does the routing and a
25 lot of mechanisms that it has, but the simple model of, you

1 know, of what I've described is -- accurately enables you to
2 answer the question of: Are you next to the requester or are
3 you next to the relayer? If it's the person who originally
4 requested the file, you would expect to see a much larger
5 number of requests and if you're, in fact, talking to a
6 relayer, you would see many fewer.

7 Q Now when the request for the blocks of the file goes out,
8 how is that information passed from the original requester to
9 its peers?

10 A So when you're the original requester and you have this
11 manifest that contains the list of blocks that you are
12 attempting to retrieve, you'll directly ask your next door
13 peer. You'll say, "Do you have this particular key I'm
14 looking for?"

15 It is a question that is directed directly at your
16 peer. It's not a letter that's destined to someone else. As
17 an analogy, it's like a chain letter that no matter who you
18 give it to, they are designed -- it's designed for them to
19 read and act on. And they may end up passing that chain
20 letter on, but it's a message that is destined for them.

21 So to make sure I answer your question, you -- the
22 requester has this manifest. It has the list of blocks it's
23 searching for. It has a routing algorithm that allows it to
24 pick one of its friends, one of its neighbors, one of its
25 peers; all the same thing. "Are you the one who might have

1 this block I'm looking for? And, by the way, after you've
2 answered that question for yourself, go ahead and ask one of
3 your neighbors. And at some point you'll fail, and let me
4 know and I'll -- I'll back off and try again at a high level."

5 Q So if the original file request goes out and one of the
6 requests for a block goes to a peer and the peer doesn't have
7 it, you know, it reads the communication, it says, "I do not
8 have this block," what happens next?

9 A They'll look at their collection of -- of peers, their
10 neighbors, and they'll select according to this routing
11 algorithm which one is most likely to have the block from the
12 information they have, and they'll select that one and then
13 they'll pass it on. And, again, that's a message directed for
14 that neighbor. They'll look at it, read it and decide if they
15 have a copy of what they need. And if not, the same process
16 continues until -- until it's decided it should stop.

17 Q Are IP addresses available or -- How do IP addresses work
18 on *Freenet*?

19 A Well, IP addresses are, you know -- "IP" stands for
20 "Internet Protocol." IP addresses are the fundamental aspect
21 of the Internet that allows us to route messages. So when you
22 join the free -- *the Freenet* network, again, it does not hide
23 what IP address you have with your neighbors who are also on
24 *Freenet*. They know directly who they're talking to, and they
25 need to because these messages are intended for their

1 neighbors to ask them if they have those blocks. It's -- It's
2 a fundamental part of the Internet. It's a fundamental part
3 of *Freenet*. It's not obfuscated in any way.

4 Q Now *Freenet* does advertise itself as a place that tries
5 to be more of a harbor for anonymity. Is that correct?

6 A Yes. It's a privacy -- It bills itself as a
7 privacy-enhancing technology.

8 Q But are there warnings that *Freenet* gives about the
9 limits to its privacy and security?

10 A Yes. As we saw, I don't -- I don't recall the number,
11 but there was an exhibit earlier today we all saw upon
12 installation. People who do install the software, as part of
13 the installation process, that warning is shown. I myself
14 have seen from -- There are further warnings that appear. If
15 you modify or look into the configurations settings of *Freenet*
16 that are presented to users, there's yet another warning.

17 My recollection is that at least at some point when
18 I -- when I went there, I didn't go today or anything, but at
19 some point on the *Freenet* website, there was also a warning
20 stating that, you know, I don't remember the exact wording, so
21 I'm just paraphrasing here, but it was, yet, another warning
22 to users that the Open Net mode, for example, is perhaps not
23 very secure at all.

24 Personally, I've looked through the mailing list of
25 the developers of *Freenet*, the software engineers who look --

1 who design *Freenet* as a volunteer effort, and they've had many
2 discussions about how this Open Net mode is, in fact, quite
3 vulnerable and doesn't provide protection very well at all.
4 We have mentioned that there's another mode of *Freenet* called
5 "Dark Net," and my -- my reading of their messages on these
6 public developer mailing lists is that they don't believe Open
7 Net is very secure at all and they wish users would move to
8 Dark Net.

9 Q Now we mentioned earlier that *Freenet* is open source or
10 the source code is open. What does that mean?

11 A "Open source" means that the program that you have
12 downloaded -- I think most users on the Internet download
13 what's called an "executable." You download it and it runs.
14 You double-click it and it runs. That's an executable, but
15 all programs on the Internet start with some sort of source
16 code typed in by a programmer or a software engineer. In
17 *Freenet*'s case the source code for the program is available on
18 the web, and so anyone who has the program -- Anyone is
19 available -- Anyone is -- It's possible for anyone in the
20 world to download not only the executable but the source code
21 for the program. And this all relates to the idea that the
22 software itself is -- is free and available for anyone to run.
23 There's no special -- Especially in Open Net mode, there's no
24 one to meet. We saw at least three screenshots today that
25 immediately upon installing, you're up and you've joined the

1 network and it's connected you to a bunch of strangers who
2 themselves, you know, either just downloaded it or have been
3 running for a while. There's no -- There's no chat room to
4 join to. There's no access code.

5 Q Since it's open source, can anyone modify their version
6 of *Freenet* in some way?

7 A Yes; yeah, anyone with -- with the skills to look at *Java*
8 of which, you know, it's an extremely popular network. I'm
9 sorry. It's an extremely popular language. It's not
10 something obscure. For example, at UMASS - Amherst the
11 majority of classes in the Computer Science major are taught
12 in *Java*, so it's a -- it's a very accessible language. It's,
13 in fact, very verbose and friendly, and so modifying *Freenet*
14 would be quite easy for any one of the -- I don't know how
15 many people in the world not only have technical degrees but
16 for whatever reason have taken the time to learn a programming
17 language like *Java*.

18 Q And Investigator Becker testified earlier that he was
19 able to make a patch for *Freenet*. What was that about?

20 A He was able to apply a patch. A patch is just a general
21 term that means since the code is open source, you can take
22 any part of it and change anything you like. And my
23 understanding is, if I recall the testimony you're referring
24 to, he was -- he was referring to a patch to the program that
25 enabled it to log extra information. And, you know, anyone

1 could have done that.

2 Q So anyone on their version of *Freenet* can do a patch
3 similar to what --

4 A Absolutely.

5 Q -- Investigator Becker did.

6 A Yes.

7 Q Now I'm going to move on to talking about specifically
8 law enforcement on *Freenet* and their search for child
9 pornography offenders. Is there a way, based on your
10 research, in order to help law enforcement find child
11 pornography offenders on *Freenet*?

12 A Yes. The analogy I gave previously about M&Ms and so on
13 is a -- is a really high-level discussion of the technique --
14 excuse me -- the technique that we developed that would allow
15 really anyone but law enforcement, in particular, to
16 distinguish the roles of requester and relayer on *Freenet*.

17 Q So the basic methodology to find offenders on *Freenet* is
18 to use that method of differentiating requesters and relayers.

19 A Yes. Using that information that's been sent to you,
20 that's -- that's directed to you by your neighbors, you can
21 look at that information and then distinguish those two roles.

22 I -- I should say there's, of course, the component
23 that was spoken of before. You need to have the manifest in
24 place first. As these -- As these -- You haven't really asked
25 me about this, so I'll just mention it.

1 Q Sure.

2 A There's another detail about knowing which blocks are
3 part of the same file that's being downloaded. You can't take
4 any blocks, you know. There's an extra step there, but -- but
5 at a high level, if I can answer your question correctly, yes,
6 that's the basic method.

7 Q Has this method ever been tested? The method that law
8 enforcement is currently using to find child pornography
9 offenders on *Freenet*.

10 A Yes. So the method that -- that I just described is
11 written down in a -- in the publication that I've described
12 that's been peer reviewed and has been described in the
13 peer-reviewed paper. We did a number of tests. First of all,
14 we have a -- a mathematical model of what we're doing. What's
15 nice about a mathematic model is it's extremely precise. I've
16 been using the best words I can here to describe what we're
17 doing but, of course, mathematics is always better. So that's
18 number one is it's very clearly described.

19 Number two, it's easy to implement this particular
20 model of -- that allows you to distinguish between these two
21 roles. And so since it's so easy, we were able to
22 construct -- we were able to construct a simulation of how
23 *Freenet* works. So if you'll allow me, let me step back here
24 and say: There's -- So I've been in research, you know, a
25 fair -- a fair bit of time now, as I've described, and there's

1 very standard ways of analyzing algorithms of this type; in
2 other words, algorithms that would come to a decision;
3 algorithms for distinguishing between a relay and a
4 requester. So I've done this across many papers; ten -- tens
5 of papers, and there's a standard method of doing that.

6 And the standard method is basically you have a
7 mathematical model and then there's perhaps something to
8 validate that mathematical model. So the way we validated it
9 was to create a simulation of how *Freenet* works. And, in
10 fact, the way -- that idea of creating a simulation of how
11 *Freenet* works is precisely what's been done in other papers
12 that have found vulnerabilities in *Freenet*. So it's quite
13 standard what we did there.

14 And so using this simulation of how *Freenet* does its
15 routing, we were able to validate the technique. And by that,
16 I mean analyzed its true positive read. And then our
17 experiments, which were quite extensive, using this
18 simulation, the true positive read was -- I don't want to say
19 it was a hundred percent but it was -- it was close to that,
20 depending on a number of factors that are described in the
21 paper.

22 Now that's not the only way to -- to evaluate an
23 algorithm is the true positive read. There's also a false
24 positive read that you have to be concerned with. So in order
25 to evaluate the false positive read of our algorithm, we

1 actually got on the network and took traces of -- of -- I'm
2 sorry. We got on the network and we looked at the messages
3 that were directed to us; that were sent to us by our *Freenet*
4 peers that we were supposed to look at, and we looked at ones
5 that we knew were not requesters.

6 Now I haven't quite explained this, but we had talked
7 a bit about the "Hops To Live" field, and let me just say this
8 little detail. A Hops To Live of 16 definitely means you're
9 not looking at the requester. So we can take messages that
10 were directed to us that have Hops To Live of 16. We know
11 that these are not requests for the file. They're not sent by
12 someone who's requested the file, and then we can run those
13 messages against our algorithm. And so when we did that, we
14 found that the false positive read was two percent, roughly.

15 So in sum, we looked at the true positive read of the
16 algorithm using a simulation which is quite standard in my
17 field to validate the mathematical model, and then we looked
18 at the false positive read by actually applying it to *Freenet*
19 data. And what's nice about that is it has ground truth;
20 right?

21 And so -- so we're -- we're quite confident in those
22 results. And those results are published now and peer
23 reviewed, and the methodology we used was completely accepted
24 by the -- by the reviewers.

25 Q Going back, can you just briefly remind us of what "Hops

1 To Live" is? Like what does that value ---

2 A Hops To Live -- When I talked before, I said you ask your
3 neighbors, "Hey, do you have this file? If not, could you
4 pass it on?"

5 There has to be an end point to that. And each time
6 you ask your neighbor, "Do you have this," and they ask their
7 neighbor, "Do you have this," in general, they're going to
8 decrement or lower by 1 that "Hops To Live" value. So it will
9 go, say, from 16 to 15 to 14. And at some point that value
10 will hit zero and you've hit a dead end and you can stop
11 because, otherwise, we'd have requests floating around on the
12 Internet forever and ever and ever, and that -- that doesn't
13 make for good networking.

14 But the high-level point is that by looking at that
15 value, we can measure the false positive rate accurately.

16 Q And you were able to do that with the method that law
17 enforcement is using to find offenders on *Freenet*, correct?

18 A We were able to do that for the method that I described
19 in the paper. And we did that for -- My recollection is we
20 did it for over 26,000 runs of data. So in other words, it
21 was about 26,000 experiments is one view of it which is quite
22 extensive, yes.

23 MS. LANG: Your Honor, at this time I'm going to ask
24 that the witness be qualified in networking and network
25 security.

1 Do you have an objection, Mr. Fein?

2 THE COURT: Is there any objection to this witness
3 being qualified as an expert?

4 MR. FEIN: I don't think so, Your Honor.

5 THE COURT: Okay. The Court will qualify the Doctor
6 as an expert in the field. And it was of computer security?

7 MS. LANG: Network security.

8 THE COURT: Network security.

9 THE WITNESS: Networks and network security.

10 THE COURT: Networks and network security. Thank
11 you.

12 THE WITNESS: Thank you, Your Honor.

13 Q (By Ms. Lang) Now we talked a lot about how -- how this
14 method has been tested and sort of generally how it works, but
15 how is the -- the count, I guess, of the requests actually
16 differentiating between the relayers?

17 A So it relates to the M&Ms example that I discussed
18 previously. There's a certain number of requests that are
19 sent out by the requester. And so say, for example, 800
20 requests -- Say there's a manifest that requires a certain --
21 Each manifest has a certain number of requests that must go
22 out from the requester. Let's say that, an example, 800 have
23 to go out. So if that peer had, say -- If the requester had
24 say, 60 neighbors, as a -- as a model for distinguishing
25 between the two roles, we might believe that an even share

1 would go to each of its neighbors; say something about 13
2 requests would go to each neighbor, if I've done the math
3 correctly. It's just hard to do up here.

4 And so each of those neighbors will look to see for
5 the message directed to them whether they have the requested
6 block. And if they don't, they're going to split it up again
7 among their neighbors. And so dividing 13 again among your
8 peers is going to be a much lower number. And so, again,
9 there's intricacies to *Freenet*, but I'm not trying to estimate
10 how many requests you receive. I'm just trying to distinguish
11 between those two scenarios. If the number is, in fact, very
12 low, it's -- it's an extremely high likelihood you're not -- I
13 mean that's a disqualifying factor. If it's -- If it's very
14 low, the number of requests you receive from a neighbor,
15 they're probably not the requester. But if, in fact, it's
16 close to an even share or even higher, then that's a high
17 likelihood that they're a requester because there's only two
18 possibilities; right?

19 They're either the requester or they're the relayer.
20 It's the only thing you need to decide between. So if one of
21 them is very unlikely, the other -- you know, and the other is
22 very likely, it's easy to do.

23 Again, I'm not trying to estimate my grade in the
24 class. I'm just trying to see whether I passed. It's an
25 easier question, and it allows for a lot of variability.

1 MS. LANG: Your Honor, may I approach the witness?

2 THE COURT: Sure.

3 Q (By Ms. Lang) I'm going to hand you what's been marked
4 as Exhibit 21.

5 A Thank you.

6 Q And 21 is -- Government's 21 is up on the screen now,
7 Dr. Levine. This is a -- The case that we're here on, this is
8 the file that was in the search warrant. And based on the
9 data that was collected by Investigator Becker and his tools,
10 it was put into this format.

11 Now if you look at, first, the timing, there --
12 there's the date and the time and the overall run time. It
13 says it's 1 minute and 58 seconds. In your opinion, what does
14 -- what does that mean? Does that tell you anything about
15 this particular request coming from this IP address to the law
16 enforcement node?

17 A Well, a minute and 58 seconds is just the time for this
18 particular -- what I would call a "run." A "run" is a
19 collection of requests. So for this run of requests, that's
20 the total amount of time that the requests were directed to
21 and received by the observing node. And so, yeah, it's a
22 minute and 58 seconds.

23 Q And then going back up, the data blocks, it says it was
24 783, and the total unique requests logged by the law
25 enforcement node was 69. Now does that tell you anything that

1 the law enforcement node got 69 requests out of a minimum of
2 783?

3 A Yeah. So before I had given my exam of 800 requesters,
4 so -- which is about what's here, just to keep the math -- I
5 don't know about simple but clear. And so if they're -- If --
6 You know, we're trying to decide is this -- given that the
7 observer received 69 requests and this file, there needs to be
8 a minimum of 783, it's just not -- it just stretches the
9 imagination to believe that this could be a relay because
10 that relay is dividing the number of blocks they have again
11 by the number of -- of -- by the number of neighbors that they
12 have. So I just can't -- It just stretches the mind to
13 believe that this could be the relay. It's just too many
14 blocks, so it's -- it's a good decision. In my mind, it's a
15 high probability, in fact, that these requests were received
16 by someone who was requesting the file; by some computer that
17 was requesting the file.

18 Q And did you independently test with this data on -- on
19 Page 1 of this exhibit?

20 A I did. I did take these exact values, and I applied it
21 to the -- The way I described the model is slightly different
22 than what's in the spreadsheet. It's a -- It's a bit more
23 precise. I mean math -- As we all know from math, there's
24 many answers to a math question, so I have a slightly
25 different one but it comes up with the same answer. In fact,

1 in my description of the problem for these set of values in
2 terms of deciding whether this is a relay or a requester,
3 there's a 98-percent -- over a 98-percent probability that
4 this is the requester of the file; that this IP address is.

5 Q And that is based on the -- on the -- your analysis using
6 the method that has been peer reviewed, correct?

7 A Yes. I used precisely the method that was described in
8 the peer-reviewed paper and came to that value.

9 MS. LANG: Your Honor, may I approach again?

10 THE COURT: Yes.

11 Q (By Ms. Lang) I'm going to hand you Exhibit 22.

12 A Thank you.

13 Q Exhibit 22 is what the Government collectively refers to
14 as the search warrant, but it also includes the affidavit and
15 application. And I want to direct your attention to Paragraph
16 6 in the affidavit in which it's written ---

17 A Hold on. Let me just -- Okay.

18 Q That Paragraph 6 there is written that -- and you can
19 probably read it -- but, "While reviewing the requests by the
20 law enforcement node on *Freenet* located in Missouri,
21 Investigator Becker observed that certain IP address," which
22 was the Defendant's, "routing or requesting suspected child
23 pornography file blocks. The number and timing of the
24 requests was significant enough to indicate that the IP
25 address was the apparent original requester of the file."

1 That second line there in that paragraph, do you
2 agree with that statement based on your analysis?

3 A Well -- So ---

4 Q Right here.

5 A Yeah. First of all, yes. More than that, you know, was
6 he the apparent original requester? That's weak. I mean if I
7 -- I'm not law enforcement. I'm -- You know, I have my own
8 job, but I would say there's a very high likelihood that this
9 was the requester. Certainly it was, you know, looking at the
10 number and timing of requests in the spreadsheet that we just
11 looked at, 783, 69 blocks requested, and the model that I
12 described and the fact that I ran it myself, it's -- this is
13 an absolutely true statement according to the model that I've
14 developed.

15 Q And then go -- On that same exhibit, if you can move to
16 Paragraph 21.

17 A Okay. Hold on.

18 Q Okay.

19 A Okay.

20 Q If you could read that.

21 A Paragraph 21 says, "This Affiant knows from training and
22 experience that streams of requests for blocks of a particular
23 file from an IP address can be evaluated to determine if the
24 IP address is the likely requester of a file."

25 Q Is that statement true? Can the requests -- streams of

1 requests of blocks be evaluated to determine who is the
2 requester of the file?

3 A Yes. And that's precisely the topic of the paper that I
4 published that is peer reviewed, and that method is reflected
5 in the spreadsheet as well.

6 Q Okay. So basically your conclusion is that what
7 Investigator Becker did in this case worked.

8 A It's not just a simple conclusion. I spent a large
9 amount of time testing the method as I said, a simulation, and
10 on real traces of -- of file -- excuse me -- on real traces of
11 packets that were sent directly to nodes on the *Freenet*.

12 MS. LANG: I don't have any other questions at this
13 time, Your Honor.

14 THE COURT: All right.

15 CROSS EXAMINATION

16 QUESTIONS BY MR. FEIN:

17 Q Good afternoon, Professor. How are you?

18 A Good afternoon.

19 Q You developed the statistical analysis that was used in
20 part in this case. Is that correct?

21 A I was one of the people that developed it, yes.

22 Q Beyond that, were you involved in the investigation of
23 the case in any other way?

24 A No. Other than, obviously, I'm here today.

25 Q Forgive me?

1 A I'm here today.

2 Q Right. You're here testifying today, but in terms of
3 Detective Becker's investigation, Detective Slaughter's
4 investigation, you played no role in any of that.

5 A I did not.

6 Q If I heard you right, you testified that the peer-review
7 process has been completed, but it hasn't been, what I'll
8 call, "certified" yet?

9 A No, I wouldn't call it "certified." It's a paper that is
10 to appear and has been officially accepted to that workshop.
11 The last stage is -- I would call it a social event.

12 Q Okay.

13 A It's informative to see papers presented by the authors
14 and not just the written word.

15 Q In April of 2015 was the method peer reviewed at that
16 point in time?

17 A No, it was not.

18 Q In June of 2015 was it peer reviewed?

19 A No. As I said, it was peer reviewed this year.

20 Q Okay. How long did -- Did you work on the statistical
21 analysis model yourself or were there other people working
22 with you?

23 A There were other people.

24 Q How many people worked on that project?

25 A About four, I guess.

1 Q I'm sorry; four?

2 A About four. Five if you include Special Investigator
3 Becker.

4 Q And how much time did it take to develop that method?

5 A Well, we had some -- We did some methods that weren't so
6 good, and so there was, I guess, an "ah-ha" moment; right?
7 And it turns out to be something we wished we had realized
8 earlier. In fact, it's quite obvious and -- and talked about
9 by the developers on the -- on the developer mailing list.
10 So, yeah, I think in the end I could have kicked myself for
11 not figuring that out earlier.

12 Q So the question is: How long did it take you to develop
13 this method that you believe works well?

14 A The answer is that I've been looking for ways to
15 investigate *Freenet* in a forensically-sound manner for a long
16 time; maybe a year, maybe two, and then this method, you know,
17 in some sense, it was developed in a moment, and then we
18 tested it.

19 The most important part of developing a method is
20 testing the true positive rate and the false positive rate and
21 defining it carefully. So that -- that was another part of
22 the process that took perhaps another year.

23 Q Okay. So this is an outgrowth of a process that took
24 place over the course of two years?

25 A Something like that.

1 Q Okay. The statistical analysis that you and the four
2 colleagues of yours developed, is that available to the
3 public?

4 A Is it available to the public? I guess not yet because
5 the site -- the ---

6 Q I'm just asking if it's available to the public.

7 A Oh, sure. I don't believe it is.

8 Q I can't buy it anywhere today if I wanted to?

9 A It's not for sale.

10 Q And just to be clear -- This is probably redundant.
11 Well, I'll even let it go. It is redundant.

12 The process by which *Freenet* functions once -- Let's
13 look at it from the perspective of someone who is requesting a
14 file. I guess even if somebody is inserting a file. Once the
15 initial insertion or the initial request through a key is
16 done, the rest of the system is automated, correct?

17 A Well, it's a piece of software.

18 Q So that would be a "yes."

19 A Yes.

20 Q So, for example, I could be running *Freenet* on my home
21 computer. I could pass away; hopefully not but I could. And
22 as long as that computer was up and running, it would still be
23 responding to requests that come through, correct?

24 A Sure.

25 Q It's an impersonal process, correct?

1 A It's a piece of software, yes.

2 Q And you testified on Direct that individuals can modify
3 *Freenet* because it's an open source piece of software. The
4 code is available, correct?

5 A Yes.

6 Q But you also indicated that they would have to have some
7 knowledge of *Java*, correct?

8 A They would have to have knowledge of the most common
9 programming language in the world, yes.

10 Q Okay. Well, it may be common and it may be the most
11 common, but you don't know how many Americans actually have
12 knowledge of using *Java*, do you, and developing code based on
13 it?

14 A I can't speak ---

15 MS. LANG: Objection; argumentative.

16 MR. FEIN: I'm just asking a question.

17 THE COURT: Overruled.

18 A I'm sorry. Can you repeat the question?

19 Q (By Mr. Fein) Do you know how many Americans have
20 sophisticated -- enough knowledge to write code in *Java* and
21 change codes using *Java*?

22 A Well -- So there's -- I don't know how many universities
23 there are in the U.S. Let's -- Let's estimate that
24 there's ---

25 Q I'm not asking you to estimate. I'm asking if you

1 know ---

2 A Do I know the exact number of people?

3 Q Yes.

4 A I don't know where that information is available for me
5 to get it.

6 Q So the answer is "no."

7 A The answer is "no."

8 Q Okay. And you teach a course at the University of
9 Amherst, right?

10 A I currently teach a course, yes.

11 Q Okay.

12 A I taught many courses in the past.

13 Q And you deal with students who are taking Computer
14 Science courses, right?

15 A I do.

16 Q Okay. I would imagine they're fairly sophisticated
17 students when it comes to Computer Science.

18 A Yeah. They're -- They're there to learn Computer
19 Science.

20 Q Not everybody has that same education, correct?

21 A Not everybody has that same education. Currently, we
22 have one of the most popular majors. There's about a thousand
23 under-grads in our program. There's, you know, several --
24 about 400 --

25 Q I'm not asking about that.

1 A -- graduate program -- graduate students as well.

2 Q I understand. Someone who doesn't know *Java* couldn't ---

3 A Well, that's a tautology.

4 Q Forgive me?

5 A The answer to that, of course, is "no." You asked it in
6 such a way the answer is "no." Someone who doesn't know *Java*
7 couldn't use *Java*.

8 Q Right. And you would have to -- you would have to know
9 *Java* to manipulate it or modify the software.

10 A If you know another programming language, you could
11 probably do a good job. *Java* happens to be very similar to
12 *Python*, all sorts of other programs.

13 Q All right. So someone in this room right now who wasn't
14 familiar with those -- those particular applications couldn't
15 modify the *Freenet* software, correct?

16 A Yes.

17 Q You indicated that you had seen on *Freenet* previously
18 warnings that you described to the Government. What year was
19 that?

20 A I don't recall the first time that I had seen those
21 warnings.

22 Q Okay. You have no idea if Mr. Dickerman saw them,
23 correct?

24 A Of course not.

25 Q You don't know if he's even the one who downloaded

1 Freenet on his computer, correct?

2 A Of course not.

3 Q Are there any terms of service on *Freenet*?

4 A I don't recall.

5 Q Did you look for any?

6 A Did I look for any terms of service? I have never looked
7 for the terms of service on *Freenet*.

8 Q The Government asked you to look at this Exhibit 22 and
9 in specific asked you about Paragraph 6.

10 A Would you mind if I opened up my draft before you ask
11 your question?

12 Q Not at all.

13 A Okay. I'm looking at Paragraph 6.

14 Q And it asked you about the term "significant enough," and
15 you were able to answer that question quite easily, correct?

16 A I believe so.

17 Q And that's based on the knowledge you have underlying
18 those two terms. That is, you had to refer to the statistical
19 information that you already know, correct?

20 A Yes.

21 Q That information is not in Paragraph 6, correct?

22 A Correct.

23 Q Looking at Paragraph 21 --

24 A Okay.

25 Q -- and there's the term "can be evaluated." And for lack

1 of a better phrase, I'll just ask: That's a proxy for can be
2 subjected to a statistical method that will yield a
3 conclusion.

4 A I -- I can only answer that: Can it be evaluated? Yes.
5 I have a peer-reviewed publication that says it can be
6 evaluated.

7 Q And that would be the method by which it would be
8 evaluated.

9 A Yes.

10 Q All right.

11 A That's one of the ways. There's probably others.

12 Q Forgive me?

13 A That's one of the ways. There might be others.

14 Q Right, there might be.

15 A Yes.

16 Q That's the one you know of.

17 A That's the one I know of.

18 Q And certainly the one at issue here.

19 A I believe so, yeah.

20 Q Do you know if requests that are sent by a requester are
21 uniformly distributed among peers?

22 A That's a very interesting question, so I've tried to
23 evaluate that question. And in the experiments that I have
24 done I wouldn't say there -- So can you rephrase the question
25 again? What precisely are you asking?

1 Q Yes. Are there -- Are the requests sent by requesters or
2 submitters uniformly distributed among its peers?

3 A So when you say uniformly distributed, you know, when I
4 hear that, I say: Is that easily modeled by what's called the
5 "uniform distribution"? Okay?

6 So that doesn't mean to me are they exactly evenly
7 distributed. It means would we expect, an expectation, would
8 they be uniformly distributed. So I've analyzed that question
9 in simulation and the answer is: They are approximately
10 uniform.

11 Q Approximately uniform.

12 A Yeah.

13 Q What is it that prevents you from saying they are, in
14 fact, uniform?

15 A They are easily modeled by a uniform distribution is a
16 better answer.

17 Q Forgive me?

18 A They are modeled well by a uniform distribution is a good
19 answer to your question.

20 Q Okay. Tell me if this makes sense: How much closer to
21 uniform does the distribution get per hop?

22 A How much closer does the distribution get to uniform at
23 each hop? I've never thought about that question, so I don't
24 know.

25 Q Okay. How did you make the determination that uniform

1 distribution is an accurate model for request distribution
2 when -- when a few hops away from the requester?

3 A In fact, what I came to the conclusion was that a uniform
4 distribution was a good model for distinguishing the relayer
5 and the requester.

6 Q How did you reach that --

7 A So, again, ---

8 Q How did you reach that?

9 A How did I reach that?

10 Q Yes.

11 A I created a model of Freenet topology and routing
12 algorithm along with my colleagues. We together created a
13 model -- a simulation rather of *Freenet*'s routing and -- and
14 topology which is something that's been done in previous
15 papers. We sent out in the model -- Without going through all
16 the details, --

17 Q Sure.

18 A -- but we sent out requests. What was a -- I mean this
19 is a simulation, so there were no actual requests here. So
20 don't -- don't mistake my meaning, but we sent out requests
21 for -- for pieces of a file and we watched where they went.
22 And then we looked at, from the simulation results which we
23 ran, you know, an enormous number of files using a compute
24 cluster, whether the distribution was about even or -- or, to
25 be more frank, whether assuming that you could model it with a

1 uniform distribution would allow you to accurately distinguish
2 the relayer and the requester.

3 So, again, I'm not trying to estimate the number of
4 requests you would get precisely but, rather, whether you can
5 distinguish these two roles.

6 Q Okay. How -- If you know, how closely did the simulator
7 reflect real world *Freenet* topology?

8 A So that's a -- that's a good question. So I think fairly
9 well, so here's why: *Freenet* is designed to approximate
10 what's -- a particular topology. It's called a "small world
11 topology." Actually relates to the whole idea of six degrees
12 of separation; that we're all connected to, you know -- Anyone
13 in the world you can find in a small number of hops. So it
14 turns out that's a particular mathematical construction. So
15 there's -- there's this idea of what *Freenet* is trying to do
16 and then there's what *Freenet* actually does. And in reality
17 people, not me but other published papers, have actually
18 looked at the topology of *Freenet* and decided whether it was
19 -- what type of -- you know, whether it was this topology or
20 that topology. So in the end, although it attempts to have a
21 particular nice topology with certain mathematical properties,
22 it edges towards this sort of lazy one. And so we evaluated
23 both as has been done in previous papers. And by running
24 both, we determined that -- that this -- you know, exactly
25 what I said; that modeling things as a uniform distribution is

1 a -- or a uniform distribution is a nice model to distinguish
2 between the relayer and the requester.

3 Q Okay. Just a quick couple of follow-up questions,
4 although I think this might already be clear in the record.

5 Data in the data stores of a *Freenet* user is
6 encrypted, correct?

7 A (Affirmative gesture). Yes. My apologies.

8 Q Forgive me; right. Users do not know what's in their
9 data store, correct?

10 A Users would not know what's in their data store unless
11 they compared it against the manifest that they had in their
12 possession.

13 Q And there are redundancies built into *Freenet*, correct?
14 So we've been talking about blocks and so on. There might be
15 multiple blocks -- same blocks stored on multiple data stores,
16 correct?

17 A Can you clarify?

18 Q Sure. So it's not as if once someone inserts a file into
19 *Freenet*, that the blocks that comprise that file are stored
20 once and only once.

21 A Oh, yes. It could be that as you request a particular
22 block, it's retrieved from, say, some far-away end point. And
23 as it is returned back to the requester, it can be placed in a
24 temporary cache. That's true.

25 Q Does the statistical model that you developed make any

1 assumptions about the ordinary functioning of *Freenet*? The
2 connections between peers and the degree to which they're
3 operating as intended?

4 A The model itself does not consider that. However, the
5 false positive test does consider that.

6 Q So ---

7 A So we talked -- The false positive test is an evaluation
8 of whether by aligning those details, the model still works.
9 And the false positive reads 2.3 percent which suggests that
10 such details are carefully considered by the model.

11 Q And the false positive tests are tests that are run to
12 make a determination about whether or not the statistical
13 analysis is working as intended, correct?

14 A (Affirmative gesture).

15 Q It's not a part -- It's not built into the statistical
16 analysis.

17 A No. Just like any forensic tool, there's a true positive
18 read and a false positive read.

19 Q Right. So when someone, for example, Detective Becker --
20 Forgive me.

21 A Oh. Go ahead.

22 Q Well, if someone, say Detective Becker, runs the
23 statistical analysis, those assumptions are built in about the
24 operating of network -- of the network. The false positive
25 test, that's not a part of what he's doing.

1 A That wouldn't be the correct thing to do. He's using a
2 model that has been tested to see whether what it includes is
3 sufficient to keep the false positive read low. So I would
4 say it is incorporated into the design of the model. It's
5 part of the testing process. So it doesn't make sense to
6 include the false positive read as a part of the test. It's
7 how you -- It's how you evaluate a method.

8 Q So ---

9 A It's not part of the method.

10 Q Okay. So your -- your point would be that anytime the
11 algorithm, the statistical analysis is operating, it's always
12 operating as it should, and it's been verified through the
13 false positive application.

14 A I would say that we tested a particular model and that
15 model tested very well, and it's acceptable to apply that
16 model.

17 Q Such that even if in a particular instance the network is
18 not operating as it should, suppose there's a loss of
19 connection, poor connections between some peers, the
20 statistical analysis will still yield these results that you
21 have a high degree of confidence in?

22 A I would say it's reasonable for someone who has been
23 trained in that method to apply the approach.

24 Q When you say "reasonable to do so," what does that mean?

25 A I think it's good practice. I think it's forensically

1 sound to apply a test -- I think it's forensically sound.

2 Sorry. Let me start again. I think it's good professional
3 practice to apply a test that's been evaluated for its true
4 positive rate and its false positive rate.

5 Q And supposing that there is a loss of connection, there
6 is some problems with peers that would not affect, as far as
7 you're concerned, the outcome of the statistical analysis.

8 A What do you mean by "affect the outcome"?

9 Q So for -- If the network isn't operating correctly and so
10 if there are individuals with poor connections and the
11 statistical analysis is run on the data that's been compiled
12 and collected, does the output of that statistical
13 analysis ---

14 A Okay. So I would say if it's obvious to the investigator
15 that everything is out of whack, then, of course, you
16 shouldn't apply the test. However, what the false positive
17 rate test we did includes is those types -- I mean this was
18 26,000 different runs over a period of months as described in
19 the paper. And during some of those months, some of these
20 things you're speculating about happened or didn't. To the
21 extent that they happened, they were captured by the test. So
22 any speculation is -- about what may or may not occur is just
23 speculation; whereas, the false positive rate test was on real
24 data with real events that happened, such as bad connections.

25 Q Sure.

1 A Now are those a problem for the test? In my experience,
2 it's a problem 2.3 percent of the time in my estimation.

3 Q How would an investigator like Detective Becker know if
4 it was a problem in a given instance if it wasn't that
5 obvious?

6 A I -- I don't know what problem you're referring to, so
7 it's hard to speculate.

8 Q The poor connections between peers.

9 A Between Professor Becker -- Excuse me. Between Special
10 Investigator Becker's peer -- node and another peer or some
11 two peers that he can't observe?

12 Q Either way.

13 A So if there was a bad connection on his computer, I would
14 think that would be obvious to him because -- You're leaving
15 this very vague.

16 Q That's true.

17 A So, for instance, if there's no Internet, I would think
18 he would realize there's no Internet. And if there's no
19 Internet between two other peers, for instance, the peer -- So
20 let me be more specific.

21 If -- If -- Put aside Special Investigator Becker for
22 a minute. Let's just talk about me.

23 Q Sure.

24 A So if I'm connected to another peer and the Internet is
25 out, I would think that would be obvious.

1 If a peer I'm connected to is -- has a neighbor where
2 the connection is down, then, fortunately, *Freenet* is dynamic
3 and will look for another peer. I mean peers come and go on
4 *Freenet* all the time; perhaps because of bad connections. And
5 a large part of the complexity of *Freenet* is to repair those
6 situations. To the extent that these problems occur, you
7 know, in the way that you're talking about, it's captured by
8 the test that we ran.

9 Q Are there ways for connections amongst peers to be
10 impaired without the network being down all together?

11 A Probably. I don't know. Can you refer to a specific
12 problem?

13 Q Well, your comment a moment ago was that, well, it would
14 be very obvious if one of the peers wasn't hooked up to the
15 Internet, so that would obvious. But aren't there ways in
16 which the connection could be impaired without the individual
17 not being connected at all?

18 A Maybe. We have to look at the source code.

19 Q You don't know.

20 A I don't know. Probably.

21 Q All right. You said you made 26,000 runs. And is a run
22 simply an instance of running the software?

23 A No. No. A run is a collection of contiguous requests
24 that, you know, for instance have the same manifest, have the
25 same HTL value.

1 Q How many runs are made on *Freenet* by users in a given
2 day?

3 A I wouldn't know.

4 Q How many in a year?

5 A I wouldn't know.

6 Q So when you say 26,000 runs and that leads you to the
7 conclusion that there is some degree of weight you can assign
8 to that number, that weight that you assign can't be compared
9 to the real world because you don't know how many runs are
10 going on in the real world in a given day in a given year.

11 A However, 26,000 runs is a good statistical number.

12 Q It sure sounds like it.

13 A So, for example, presidential elections are -- You know,
14 any sort of survey done of the public is done of a good number
15 of people when you're estimating things. This is -- This is
16 the basic of -- the basis of statistics is to take a small
17 sample of something and then make a reasoned conclusion to the
18 best of your availability following the formal model
19 statistics that's been available for hundreds of years.

20 So although I can't compare it, as you said, to the
21 real *Freenet* network, I believe I'm making a sound statistical
22 conclusion about the efficacy of the test.

23 Q Right. And what you're saying is the larger the sample
24 size, the better -- more likely it is to produce a good
25 result.

1 A Yeah. To the extent that statistics is what statistics
2 is.

3 Q Right.

4 A Right.

5 Q And it's easier to evaluate the predictive validity of a
6 particular statistical model the larger the sample -- when you
7 know that it is, in fact, a large sample size as opposed to a
8 small sample size.

9 A Twenty-six thousand is a very large sample size.

10 Q But you don't know how many runs there are in a given
11 day.

12 MS. LANG: Objection; asked and answered.

13 THE COURT: Sustained.

14 Q (By Mr. Fein) One last question: Were any changes
15 implemented to the statistical analysis based on the
16 peer-reviewed process?

17 A None at all.

18 MR. FEIN: Thank you. I have no further questions.

19 I have no further questions, Your Honor. Thank you.

20 THE COURT: Okay. Do you have any Redirect?

21 MS. LANG: I do, Your Honor, briefly.

22 REDIRECT EXAMINATION

23 QUESTIONS BY MS. LANG:

24 Q Dr. Levine, do you still have Exhibit 21 in front of you?

25 A I do.

1 Q If you could take a look at that exhibit again. On Cross
2 Exam there was some discussion about possible poor
3 connectivity between peers. In this case, the Defendant's
4 peer or the Defendant's IP address had approximately 56. -- or
5 had an average of 56.9 peers. Assuming a couple of those
6 maybe had some bad Internet connection or were going on- and
7 offline, what would -- how would that change the Percentage of
8 Even Share or change your idea about this particular Defendant
9 being the requester?

10 A Okay. So this gets back to my answer about -- I'm sorry
11 to be a little repetitive, but this gets back to my answer --
12 to my statement that we're estimating whether the role is that
13 of a requester or a relay. We're not trying to estimate
14 exactly how many requests we should have gotten and so on.
15 And so the idea that the -- Even if -- To answer your question
16 more directly, even if some -- more than a few of the 56 or 57
17 peers were down or had bad connections or were avoided by this
18 intermediary, it's just highly, highly unlikely that, as a
19 relay, 69 requests could have been sent to this observer
20 because if there had been an original requester, they would
21 have had to have sent just a unbelievable proportion of those
22 requests to this intermediary. You just can't get to those
23 numbers if you go down from 56 by quite a few.

24 So because we're answering the easier question, it's
25 very -- you know, it's very amenable to any sort of connection

1 failures that might have happened.

2 In addition, *Freenet* is constantly trying to repair
3 these connections. So the technique is quite good in that
4 sense. And that's -- that's where its accuracy comes from
5 because it doesn't need to concern itself with those problems.

6 MS. LANG: I don't have any other questions,
7 Your Honor.

8 THE COURT: All right. All right. You may step
9 down.

10 THE WITNESS: Thank you, Your Honor.

11 MS. LANG: At this time the Government has no further
12 evidence.

13 THE COURT: All right. Mr. Fein?

14 MR. FEIN: Your Honor, I just have one witness, and I
15 believe he will be here outside.

16 THE COURT: Okay. All right.

17 (The Witness, JUDGE JOHN BORBONUS, Is Sworn.)

18 THE COURT: Good afternoon, Judge.

19 DIRECT EXAMINATION

20 QUESTIONS BY MR. FEIN:

21 Q Good afternoon, Your Honor.

22 A Good afternoon.

23 MR. FEIN: Your Honor, may I approach the witness?
24 I'd like to provide him with Exhibit 22.

25 THE COURT: Yes, you may.

1 Q (By Mr. Fein) Do you have before you Exhibit 22?

2 A I do, yes.

3 Q Can I ask you briefly, Your Honor: Where did you go to
4 college?

5 A I went to undergraduate school at George Mason University
6 in Fairfax, Virginia, and --

7 Q And what ---

8 A -- law school at St. Louis University.

9 Q What was your degree in in college?

10 A Political Science.

11 Q Do you have any Computer Science background?

12 A None.

13 Q Have you taken any technology courses?

14 A No.

15 Q And I think before you is Exhibit -- Government's Exhibit
16 22. Is that correct?

17 A That is correct.

18 Q And that exhibit, if you take a moment, it consists of
19 three documents, I believe.

20 A It appears to be three separate documents, yes.

21 Q And the first document is the search -- is a search
22 warrant. Is that correct?

23 A That is correct.

24 Q The second document is an application for that search
25 warrant?

1 A Correct.

2 Q And the third document is an affidavit in support of that
3 search warrant.

4 A Correct.

5 Q So I'd like to direct your attention to the search
6 warrant first.

7 A Okay.

8 Q And that document consists of two pages, correct?

9 A That is correct.

10 Q And at the top on the far right there is a file stamp,
11 correct?

12 A Yes.

13 Q And that file stamp says August 18th, 2015?

14 A Correct.

15 Q There's also a division number?

16 A Correct.

17 Q What's that division number?

18 A 35.

19 Q Is that your division?

20 A That is my division.

21 Q And it was at that time?

22 A Yes, sir.

23 Q Going down to the first full paragraph of the search
24 warrant, there is a handwritten date.

25 A Correct.

1 Q Did you write that date in?

2 A I did.

3 Q And there's a name?

4 A My name, and I wrote that in.

5 Q Okay. And the division number as well?

6 A Correct.

7 Q And I'll direct your attention to the second page.

8 A Okay.

9 Q Is that your signature at the bottom?

10 A It is.

11 Q And there is a time that is listed on there, correct?

12 A Yeah, 14:05.

13 Q Okay. And when you fill these documents out, you're
14 careful with them, I take it.

15 A Of course.

16 Q You're a judge, and you're signing search warrants, so I
17 would assume that's something you pay attention to and take
18 with seriousness.

19 A Absolutely.

20 Q So I'll direct your attention -- Well, one moment.

21 (Pause)

22 Q (By Mr. Fein) Okay. Let's take a look at the application
23 for the search warrant.

24 A Okay.

25 Q And, again, this is -- consists of two pages. Is that

1 correct?

2 A Yes, sir.

3 Q And there is a -- There are three signatures on Page 2,
4 correct?

5 A Yes.

6 Q The first signature would be that of -- I don't know if
7 you can make it out -- Detective Slaughter?

8 A It certainly appears to say that. I don't know. I'm not
9 that familiar with Detective Slaughter's signature, so I
10 couldn't swear that that was his.

11 Q Understood. Your -- Your signature is on this document.

12 A My -- My signature here and the Prosecuting Attorney
13 Teresa Bomkamp as well.

14 Q And the date is also there.

15 A Yes, August 18th.

16 Q And, again, there's a time listed, correct?

17 A Correct.

18 Q And what is that time?

19 A 14:05.

20 Q That's the same time as on the search warrant, correct?

21 A Correct.

22 Q Okay. Let's take a look at the third document. And if
23 you'd like, you can review that for a moment.

24 A Okay.

25 Q Do you have any independent recollection of signing off

1 on this warrant?

2 A Absolutely none.

3 Q Do you have a typical practice that you follow when you
4 sign off on warrants?

5 A During this time period, I had been assigned to the
6 Associate Criminal Division, so we -- at that point I was
7 doing them on a very regular basis. Prior to that, I would
8 only get them when I was the duty judge for the week.

9 So I don't know that I had a real particular
10 procedure I would follow until I moved into that division in
11 which I was doing probably, on average, 20 search warrants a
12 week. So by that point I probably started developing a real
13 practice on it, yes.

14 Q Okay.

15 A And at this point I had been in that division
16 seven-and-a-half months.

17 Q Okay. And just to quickly -- If you turn to the last
18 page of that affidavit, again, that bears your signature?

19 A It does.

20 Q And there's also a date?

21 A August 18th at 14:05.

22 Q So that's the same time that's listed in the search
23 warrant and in the application.

24 A Correct.

25 Q Have you been involved in cases that involve digital data

1 and computer forensics in terms of signing off on search
2 warrants?

3 A I'm not sure I understand your question.

4 Q Sure. How many search warrants have you signed off on
5 that involve cases that relate to digital data and computer
6 searches, computer-based investigations?

7 MS. LANG: Objection; relevance.

8 THE COURT: Overruled.

9 A I can't -- I couldn't begin to give you a number. I
10 would tell you that in your typical -- The times that I would
11 see them would be in child pornography cases and occasionally
12 on -- And, again, if we're going to broaden the term of
13 "digital data," cell phone --

14 Q Sure.

15 A -- searches, Facebook, I mean all those sorts of things.
16 So in that situation it was rather frequent.

17 Q Okay. And what about peer-to-peer software?

18 A The peer-to-peer that I recall usually were related to
19 child pornography cases. And I would say in the six years
20 that I've been a judge or almost six years I've been a judge,
21 I've probably done 15 to 20.

22 Q Okay. Do you recall the software involved in those
23 investigations? For example, like *Limewire*?

24 A I don't remember the name of them. I remember they had
25 changed over time, I think, and the one that sticks out and

1 mostly just because I read it in here was *Freenet*. But I
2 remember prior to *Freenet* there was another one that you would
3 see for a while. And as I understood it, the peer-to-peer
4 software would change over time. I don't know if that was a
5 result of those who were using it being -- trying to stay one
6 step ahead of law enforcement, but that was -- it would change
7 is my understanding, but I have absolutely no firsthand
8 specific knowledge of any of that.

9 Q Okay. Do you know how *Freenet* functions?

10 A No.

11 Q And I take it when -- in any case, whether it's --
12 relates to digital data or narcotics, when the officers come
13 in, they present you with the materials; you review them and
14 you sign off on them, but you don't have conversations in
15 addition to the application and affidavit they provide to you.

16 MS. LANG: Objection; leading.

17 MR. FEIN: I can rephrase that.

18 THE COURT: Please rephrase.

19 Q (By Mr. Fein) When they -- When you meet with officers
20 who come in to present you with warrants, do you discuss
21 matters outside the contents of the warrant with them related
22 to the case?

23 A I would have them -- And this would be a good example of
24 one. Often the -- these types of cases had long affidavits
25 because there was a lot of language in there that for whatever

1 reason was required. I would have them, as I was reading it,
2 also talk to me about what they had done. But I would -- I
3 would read it, and there were always a few paragraphs that
4 were more important to me than others. Some of it was often
5 boilerplate stuff with regard to, you know, where you have
6 these what appear to be codes and stuff. But I would look at
7 the times that the -- that were related in here, and I would
8 pay particular attention to the sort of facts specific to each
9 one. But by the same token, they would also be talking to me
10 about what they were doing.

11 Q So do you recall if in this particular case you spoke
12 with anybody outside the affidavit?

13 A I have no recollection whatsoever. I don't know if this
14 was walked through just with the law enforcement officer, if
15 the prosecutor was with them which on occasion they would be
16 and other times wouldn't be. I have absolutely no
17 recollection.

18 MR. FEIN: Your Honor, may I approach the witness?

19 THE COURT: Sure.

20 Q (By Mr. Fein) I'll refer to this as Defendant's Exhibit
21 D as in "David." Well, I can remark it as "A," Your Honor,
22 because there isn't an "A", "B" or "C."

23 THE COURT: Okay.

24 MR. FEIN: So I'll remark it as an "A."

25 A "A"?

1 Q (By Mr. Fein) Yes.

2 A All right. It says "D" but I'll -- I'll note it as "A."

3 Q Forgive me. That's my fault.

4 A No problem.

5 Q So this is a Missouri state statute, and I take it you're
6 familiar with many Missouri state statutes.

7 A I have them all memorized.

8 Q Well, I aspire to that degree of knowledge.

9 I direct your attention to Subdivision (3), and this
10 particular statute is RSMo 542.276.1, and I just ask you to
11 take a look at Subdivision (3), and go ahead and read that to
12 yourself. You don't have to read it out loud.

13 (Pause)

14 A Okay.

15 Q So that -- Do you note anything about whether or not it's
16 appropriate under Missouri state law to take oral testimony in
17 connection with the issuance of a search warrant, given
18 Subdivision (3)?

19 A I mean certainly it states in Subdivision -- in
20 Subsection (3) that oral testimony shall not be considered.

21 Q Correct. Which means that when a warrant is signed off
22 on, you have to rely on the warrant itself, correct?

23 A Correct.

24 Q Or to make that -- My phrasing is poor. You have to rely
25 on the application and the affidavit.

1 A Correct.

2 Q Okay. And I presume you would follow the law of the
3 state.

4 A I always try to.

5 Q That said, let me direct your attention to the affidavit
6 again and Paragraph -- let's take a look at Paragraph 6, and
7 if you'd take a moment to read that to yourself. Again, this
8 would be Exhibit 22, Government's 22.

9 A Okay. I've had an opportunity.

10 Q What is a "block"?

11 MS. LANG: Objection, Your Honor, to relevance; this
12 whole line of testimony. The Judge signed the warrant back in
13 2015 after reading it. There's no foundation being laid that
14 there is anything improper about the underlying signing of the
15 search warrant.

16 MR. FEIN: If you read my motion, the motion is that
17 this is a particularly technical matter, and I do not believe
18 the Judge had the wherewithal to understand everything about
19 it. And as you know, there is case law from the U.S. Supreme
20 Court and the Federal Courts of Appeal that indicates if a
21 judge cannot follow through on his duty to be neutral and
22 detached, that that is grounds to suppress evidence, and the
23 Good Faith exception to the warrant requirement would not
24 apply in those circumstances.

25 So to argue, as the Government does, that a judge's

1 basis of knowledge for signing off on a warrant is irrelevant
2 to a search-and-seizure matter would seem to be beyond
3 credulity to me.

4 THE COURT: The question you're asking does not have
5 anything to do with his being neutral or detached. And the
6 Judge's signing of the warrant has to do with whether or not
7 the Judge found probable cause to believe that this warrant
8 should be signed. So does this question go to his probable
9 cause finding?

10 MR. FEIN: So it would go to two things, Your Honor.
11 One, how could -- So I disagree with the Court's
12 characterization for the following reason: The Judge -- A
13 judge has to be neutral and detached; that the judge simply
14 isn't rubber-stamping law enforcement activities. If a judge
15 does not understand the material in the warrant, and this has
16 nothing to do with this particular judge, there are lots and
17 lots of articles about the difficulty that the legal community
18 is experiencing with highly-technical matters, and I would
19 argue this is one instance of that. And if it couldn't be
20 understood but it was authorized, anyway, then in that
21 particular event it would be a rubber stamp for law
22 enforcement and not signed off on by an individual making his
23 own determination about the facts that support probable cause.

24 MS. LANG: Your Honor, the criminal justice system
25 relies on juries, judges and Grand Juries, all of whom do not

1 have advanced computer or technical expertise but can still
2 look at facts, understand them, and then apply the law
3 accordingly or determine whether or not there's probable cause
4 in a case.

5 There's no indication in this case from the motions
6 that Mr. Fein has filed that there is anything improper with
7 the signing of the search warrant, and the case law is direct.
8 It only goes to, you know, whether a judge has a conflict of
9 interest. A bias cannot be capable of neutral. There's no
10 case law that says that -- about a -- about a judge having had
11 to have a Computer Science degree in order to sign a *Freenet*
12 search warrant.

13 THE COURT: I mean that, I guess, is a bit of my
14 concern, Mr. Fein. We ---

15 MR. FEIN: Two things, Your Honor.

16 THE COURT: Yes.

17 MR. FEIN: So the Government says there's no
18 indication anywhere that the Judge failed to have the
19 requisite knowledge. Well, obviously, if I can't develop that
20 evidence, I wouldn't expect it to be in the discovery because
21 the discovery consists of a police report, some forensic
22 reports. I would not expect that discovery to tell me
23 anything about the Judge's wherewithal with respect to a
24 warrant he signed off on. The only way to develop that
25 evidence would be to do it here today.

1 Number two, I'm not arguing that a judge needs a
2 Computer Science degree, but what I am saying is that law
3 enforcement has an obligation to present to judges
4 applications and affidavits for search warrants that allow
5 them to make determinations.

6 Now if we don't want to turn a blind eye to it and
7 say, "Everything is fine and we'll keep proceeding as we are,
8 and no one really needs to catch up with technology," that's
9 fine, but people wind up in jail over these determinations and
10 go to prison over these determinations. So I would suggest
11 it's somewhat serious. And if I can only develop the
12 testimony in this way, that is the way it ought to be
13 developed.

14 Further, the case law says a rubber stamp for law
15 enforcement -- Now that doesn't -- I'm not shooting anyone's
16 integrity. It's simply acknowledging that we're living in a
17 changing world where information is difficult to grasp. And
18 when that happens, law enforcement can't necessarily proceed
19 as they always have which I will show in a moment exactly what
20 I mean; that we have to make changes so that those who are in
21 positions of authority to make determinations about whether or
22 not individuals, like Mr. Dickerman, are restrained or
23 deprived of their liberty for many years potentially, that the
24 process is functioning.

25 Now if we are going to insulate from examination the

1 individuals who are players in that system, that's fine, but
2 we'll all have to acknowledge that we're not doing our job.
3 What we're doing is we're shielding one another from actually
4 making sure that the process is functioning as it's designed
5 to. The Government would say, "This is beyond any -- beyond
6 any question. If a judge signs off on it, that's it."

7 That is not the case, and I have very good reason to
8 believe, based on what I believe is a very technical matter
9 and a very difficult matter to understand, that the Judge was
10 not presented with sufficient information for him to make a
11 probable cause determination; not because he's deficient in
12 some way but because the affidavit simply doesn't give that
13 information. I couldn't make sense of this without the help
14 of many, many people to help me understand this. Much of the
15 information didn't even come to light till today, and I
16 suggest to the Court that the good Judge would be in the same
17 position. And the only way to find that out would be to ask
18 some questions about that affidavit.

19 Now if the Court wants to insulate him from Cross
20 Examination or discussion about those matters, I suspect
21 that's the Court's prerogative. I'll object and I'll take it
22 up with an appellate court on down the road, but that is --
23 seems to me we can't insulate the system from scrutiny because
24 we just don't like it.

25 MS. LANG: Your Honor, if the defense believes that

1 this Judge acted as a rubber stamp in this particular case,
2 then I believe those are the lines of questioning he needs to
3 go down with the Judge; asking him if he did, in fact, sign
4 the warrant with -- with no other reason but to collude with
5 the police and be a rubber stamp. Actually asking the
6 technical questions about how the program works I don't
7 believe is relevant to this Judge at this point. If he
8 believes that the search warrant doesn't fully explain what it
9 should, then he needs to attack the search warrant affidavit
10 and the four corners of the warrant, and I believe that's the
11 whole reason we're actually here in court today. Asking this
12 Judge particular questions, I believe, is actually invading
13 the province of this Court whose job is to determine whether
14 or not with the search warrant, a judge could have found
15 probable cause.

16 MR. FEIN: I disagree because the case law is quite
17 clear that when a judge cannot perform as a neutral and
18 detached Magistrate and performs as a rubber stamp for law
19 enforcement, that that is a matter that leads to suppression
20 of evidence. So I'm being repetitive.

21 THE COURT: I guess that's -- I guess that is where I
22 have a bit of a concern here is that you're making an
23 allegation that the Judge has acted as a rubber stamp, and I
24 don't -- I don't know if this -- how this line of questioning
25 is getting you to -- to that conclusion. I guess that's

1 where you --

2 MR. FEIN: Let me explain.

3 THE COURT: -- you just go to he's not neutral and
4 detached. And I'm not -- I am not here to protect anyone.
5 That is not the point here. I want -- I agree with you that
6 this is a very complicated situation. This -- This is a
7 complicated area. *Freenet*, I've -- I have spent a lot of time
8 myself learning about it because what it comes down to is
9 whether or not the search warrant that was presented to the
10 Judge provided enough information for him to make a probable
11 cause determination. So I think -- I agree with Ms. Lang
12 that -- some questions along that line before going into
13 defining every term that's in the search warrant.

14 MR. FEIN: Well, Your Honor, how -- how can I ferret
15 out whether or not he understood what was in there without
16 asking him if he understands what the words mean?

17 For example, suppose you were presented with a
18 warrant that was signed off on by a judge. This is certainly
19 no offense to the Judge. I don't know him, and I have every
20 reason to believe he's thoroughly decent and doing the best he
21 can. Suppose it was written in Greek and signed off on by a
22 Judge. Would I have no right to question that judge whether
23 or not he understood the Greek terms in the affidavit or the
24 application?

25 THE COURT: You could ask him whether he understood.

1 Maybe he was a judge who understood Greek. I don't know.

2 MR. FEIN: Well, this is why I asked him what a
3 "block" is.

4 THE COURT: Okay. If you -- How about a more general
5 question?

6 I'll allow some questions here. Okay?

7 I just am wondering -- I don't want to get bogged
8 down in asking about every technical term here because I don't
9 know if that means that he doesn't understand how *Freenet*
10 operates, how nodes operate and generally what was the
11 allegation in the search warrant which was that because of the
12 methodology that they used, this IP address was more likely --
13 I can't remember what the terminology is but was ---

14 MR. FEIN: Bear that in mind.

15 THE COURT: Huh?

16 MR. FEIN: Bear that in mind.

17 THE COURT: I can't -- Well, I can't because I'm not
18 reading the search warrant right now.

19 MR. FEIN: Right.

20 THE COURT: But when I do read them, I pay attention
21 to them.

22 MR. FEIN: Right; sure. I'm sure all do.

23 THE COURT: But I'm just -- But what I'm saying is:
24 He was presented with a search warrant that had -- had a
25 conclusion in there. So it comes down to how much

1 information -- Do I need to know how -- how methamphetamine
2 works for me to sign a search warrant involving
3 methamphetamine?

4 MR. FEIN: Let me give an example.

5 THE COURT: I guess that's my concern here.

6 MR. FEIN: Let me give an example. Let me give an
7 example. Okay?

8 Let's suppose I -- And I can do this through
9 questioning right now and avoid the example, but if you want
10 me to give an example, I will.

11 Let's suppose that an officer came to you and asked
12 you to sign off on a warrant for a home and told you because
13 that officer believed -- suspected there was drug transactions
14 occurring from within that home, and the officer told you, "I
15 surveilled the home and I saw people there, and the number I
16 saw was significant enough over a time period." Would you
17 sign off on that, Your Honor?

18 THE COURT: He has a good point there. Probably not.

19 MR. FEIN: That's correct.

20 MS. LANG: Well, I think the search warrant, as in
21 this affidavit, goes on to say not just the number and timing
22 of what's going on but that a request for this -- this --

23 MR. FEIN: Well, let me ask the questions.

24 MS. LANG: -- this legal -- this legal ---

25 THE COURT: I will allow him to ask some questions,

1 and -- and your objections will be noted. Okay?

2 MR. FEIN: Thank you, Your Honor.

3 Q (By Mr. Fein) And again, Your Honor, I -- I mean no
4 offense to you.

5 A None is taken.

6 Q But these are complicated matters, --

7 A I understand.

8 Q -- and this is important to a gentleman that I'm
9 representing.

10 A I understand, sir.

11 Q Your Honor, if you -- At some point I would go back to my
12 first question if you're going to ---

13 THE COURT: Go ahead.

14 Q (By Mr. Fein) So, Your Honor, do you know what a "block"
15 is?

16 A As used herein? No.

17 Q Do you know what a "key" is?

18 A As used herein?

19 Q Yes.

20 A I'm trying to find where I would see the word "key."

21 Q Oh, forgive me, Your Honor. That's my fault.

22 A Okay.

23 Q If you look at Paragraph 4 and Paragraph 5, the word is
24 used in those two locations.

25 A I do not.

1 Q I'm going to direct your attention to Paragraph 6, and I
2 think I asked you to read a moment ago. I'll ask you to read
3 it again because there's been a lot of back and forth, and you
4 might have forgotten it by now. I know I've tried to.

5 A Okay.

6 Q I'm going to direct you to the last sentence in that
7 paragraph, and I'll just read that one out loud. It says,
8 "The number and timing of the requests was significant enough
9 to indicate the IP address was the apparent original requester
10 of the file."

11 What does "significant enough" mean, Your Honor?

12 A Are you asking me to define the phrase "significant
13 enough"?

14 Q I'm asking you. What probability could you attach to
15 just the phrase "significant" -- Can you attach any
16 probability to the phrase "significant enough"?

17 MS. LANG: Objection, Your Honor; it's just
18 argumentative. It's simply invading the province of this
19 Court.

20 THE COURT: I will sustain the objection.

21 Q (By Mr. Fein) If you were going -- Your Honor, if you
22 were going to sign off on a warrant for a home where there is
23 an officer who said, "I've been surveilling this home and I've
24 watched drug activity; I've seen individuals come and go from
25 that home," and the application said that, "The number of

1 individuals I've seen is significant enough," but didn't tell
2 you how many, over what duration of time, over what time of
3 day, over how long they stayed, would you sign off on that
4 warrant?

5 MS. LANG: Objection, Your Honor, to this
6 hypothetical. I believe it's improper.

7 THE COURT: I'll sustain the objection. I get your
8 point, Mr. Fein.

9 Q (By Mr. Fein) I'm going to direct your attention to
10 Paragraph 7.

11 A Okay.

12 Q And if you look at the -- Well, go ahead and read it,
13 Your Honor. Forgive me.

14 A You want me to read it out loud or just to myself?

15 Q No, no; just to yourself.

16 A Okay.

17 Q And just let me know when you're done.

18 A Okay.

19 Q If I read that right, Paragraph 7 indicates that there
20 were 69 blocks, parts, blocks of a file that were identified
21 in Paragraph 7, correct?

22 A It says, "There were 69 parts or blocks of the following
23 file," and then it sets forth what that is.

24 Q Does the affidavit tell you anywhere how many blocks in
25 total that file was comprised of?

1 A Can you repeat the question?

2 Q Sure. Does the -- Do any of the paragraphs there, 6 or
3 7, indicate to you how many blocks in total the file was
4 comprised of?

5 So if you've got 69, what's the total number of
6 blocks? Is that in there?

7 A It speaks for itself. I'm not sure I understand the
8 question. It says 69 parts or blocks.

9 Q Fair enough. It just says 69 blocks, right?

10 A Well, actually it then goes on to talk about 17 JPEG
11 images containing ---

12 Q Correct. But those are -- Do you understand the
13 relationship between those blocks and the 17 files?

14 A It says 17 images.

15 Q Okay. Do you understand the relationship between those
16 17 blocks and -- I'm sorry -- between those 69 blocks and the
17 17 images?

18 A No.

19 Q Okay. And when I ask you the question how many blocks
20 comprise the entire file, does that question mean anything to
21 you?

22 MS. LANG: Objection, Your Honor, to this line of
23 questioning.

24 THE COURT: I'm sorry?

25 MS. LANG: Objection to this line of questioning.

1 MR. FEIN: I just asked him if that means anything to
2 him.

3 THE COURT: I thought he -- You -- That's right; you
4 asked him how many blocks, --

5 MR. FEIN: Right.

6 THE COURT: -- and he said, "No, it's not in there
7 anywhere." Okay.

8 MR. FEIN: I'm just asking if that means anything to
9 him.

10 MS. LANG: Asked and answered, I guess.

11 THE COURT: Overruled.

12 A I can tell me you that on this paragraph, it's probably
13 the portion under "Description" which meant something to me.
14 The rest of it might as well have been written in Greek --

15 Q (By Mr. Fein) Okay.

16 A -- because I don't understand what blocks are or how the
17 JPEG image files are related to the blocks or anything like
18 that.

19 Q All right.

20 A But what I did take from this paragraph was that 17
21 images of what appeared to be child pornography were
22 discovered.

23 Q Right. And you took that on -- You took that as it was
24 written, right?

25 A Correct.

1 Q But the -- You took that conclusion as it's stated there.

2 A Okay. I did not see the images, yes, so I relied simply
3 on ---

4 Q Yeah. I don't mean you would have seen the images, --

5 A Right.

6 Q -- and I don't expect that. I just mean there's a
7 conclusion and you accepted that conclusion, but the
8 foundation, the data underlying that conclusion, was Greek to
9 you.

10 A Correct.

11 MR. FEIN: I have no further questions, Your Honor.

12 THE COURT: All right.

13 CROSS EXAMINATION

14 QUESTIONS BY MS. LANG:

15 Q Do you know the Defendant in this case, Mr. Dickerman?

16 A I do not.

17 Q Do you have any indication that you were working in
18 collusion with the police to somehow frame Mr. Dickerman in a
19 crime?

20 A I have no such indication.

21 Q Now I'm going to go through this affidavit with you, but
22 I'm going to start -- and I'm going to assume you read the
23 whole entire affidavit before you signed it, correct?

24 A I would say that I -- I read the whole thing as I was
25 reviewing it. I would tell you that there was much that I

1 probably glazed over in the sense of what we just have been
2 talking about, but, yes, I read the entire affidavit. I read
3 the entire affidavit. The warrant is boilerplate, so I don't
4 typically read that. I do look closely to make sure the
5 language is somewhat with the address, but, yeah, I read the
6 entire affidavit.

7 Q So I'm actually going to start back at Page 12 -- excuse
8 me -- Paragraph 12.

9 A Okay.

10 Q And it states -- It talks about *Freenet*, and it states
11 that *Freenet* basically is a peer-to-peer network. It lets
12 users anonymously share files. It's a free software. It's
13 publicly available, and its communications are running on
14 *Freenet* that are nodes, and they're running between people
15 that are on this peer-to-peer network.

16 Now if you go to Paragraph 13, isn't it true that it
17 talks about how files that are stored in *Freenet*, like files
18 of child pornography, use a key to create a digital --
19 compressed digital representation method called a "SHA" or a
20 "Secured Hash Algorithm"? Have you heard of "SHA" before,
21 that term?

22 A "SHA"?

23 Q Yes.

24 A No.

25 Q The "Secured Hash Algorithm," SHA.

1 A I -- I can tell you I've heard of it.

2 Q Okay. You've heard of that term before?

3 A Yes.

4 Q And in Paragraph 14, isn't it true that it talks about
5 blocks, and it explains that *Freenet* breaks a file into small
6 pieces or blocks which have their own unique key based on a
7 SHA value?

8 MR. FEIN: Your Honor, if she wants to ask a
9 question, that's fine, but just to read the affidavit to him
10 seems somewhat peculiar to me.

11 THE COURT: She asked a question after No. 13 and now
12 she's at No. 14.

13 MR. FEIN: Very good, Your Honor.

14 THE COURT: You had a lot of leeway there. I'm going
15 to allow her some.

16 MR. FEIN: Fair enough.

17 Q (By Ms. Lang) So Paragraph 14, it explains what blocks
18 are. They're small pieces of a file, correct?

19 A Correct.

20 Q It states it right there. And it also talks about keys.
21 It also talked about keys above in Paragraph 13 and defined
22 what those were, correct?

23 A Correct.

24 Q And in Paragraph 14, it also says, you know, that the
25 keys to all parts of the file are found in a high-level index

1 block also called a "manifest," correct?

2 A Correct.

3 Q And then 15 talks about an IP address, and I'm assuming
4 you've heard of what an IP address is before, correct?

5 A I do know -- I do; I have.

6 Q And it talks about how IP addresses can be used to
7 determine who is the person, you know, behind what's going on
8 online, correct? Or it goes to the address.

9 A My understanding ---

10 Q An IP address is an identifier.

11 A It's an identifier, not necessarily as to a person but to
12 a computer.

13 Q Correct. Thank you. And Paragraph 16 talks about how
14 *Freenet* receives requests from other computers running that
15 same program, and it talks about how those requests contain a
16 key to retrieve that -- the file or a part of the file.

17 A Correct.

18 Q And Paragraph 17 talks about how *Freenet*, as a
19 peer-to-peer network, attempts to hide what a user is
20 requesting, including whether -- especially, you know, when it
21 comes to collecting or sharing child pornography files, and
22 it's not a significant source of music. That's described for
23 you; just a little information, correct?

24 A Correct.

25 Q In 18 it talks about how *Freenet* sends requests to peers

1 for blocks of files that they are attempting to download,
2 correct?

3 A Correct.

4 Q And then 19, again, it continues to explain how the
5 *Freenet* network works and how files of child pornography can
6 be obtained, correct?

7 A Correct.

8 Q And 20 talks about how someone who is requesting these
9 blocks of a file has taken substantial steps to install
10 *Freenet* and locate the key to download that file. Is that
11 correct?

12 A That is correct.

13 Q How -- How a person finds a file on *Freenet* is basically
14 what it's talking about.

15 Paragraph 21 talks about how you can evaluate the
16 streams of requests for a block of a particular -- blocks of a
17 particular file from an IP address to determine if that IP
18 address is likely the requester of the file. Is that correct?

19 A That is correct.

20 Q And then 22 talks about how child pornography offenders
21 typically act, and 23 also talks about that. Is that correct?

22 A That is correct.

23 Q So there's multiple paragraphs in the search warrant that
24 explain what blocks are, what keys are, what *Freenet* -- how
25 *Freenet* works, and how you find files, including files of

1 child pornography on this network, correct?

2 A Correct.

3 Q Is there a date of a crime that occurred? Or actually
4 let me just direct -- I'll just direct you.

5 On Paragraph 7, isn't it correct that on April 2nd,
6 2015, S.I. Becker, Investigator Becker, located a request for
7 a file of known child pornography, correct?

8 A Correct.

9 Q So there you have a date and the crime. Requesting child
10 pornography is illegal, correct?

11 A Correct.

12 Q And it has an IP address that was associated to that
13 request of child pornography listed in Paragraph 7, also;
14 correct?

15 MR. FEIN: I object. There's an IP address that's
16 alleged to be ---

17 THE COURT: She said an IP address was listed --

18 MS. LANG: In the search warrant.

19 THE COURT: -- in the search warrant and, yes, it is.
20 And I'll overrule your objection.

21 Go ahead, Ms. Lang.

22 MS. LANG: Thank you.

23 Q (By Ms. Lang) And then going down to Paragraph 9, the
24 affidavit explains that that particular IP address, they were
25 able to determine, through AT&T, went to a particular address

1 at 9524 Corregidor Drive. Is that correct?

2 A That's correct.

3 Q So now you have a crime, a date and a place --

4 A Correct.

5 Q -- where the crime has alleged to have occurred in the
6 affidavit.

7 A Correct.

8 Q So if you had an affidavit where you have a place where a
9 crime occurred, a date where it occurred and what type of
10 crime is occurring there, that would be enough information to
11 form probable cause, correct?

12 MR. FEIN: Objection, Your Honor. It's a
13 hypothetical.

14 THE COURT: I'm sorry?

15 MR. FEIN: It's a hypothetical; "if you have." It's
16 sustained as to my question earlier.

17 THE COURT: I will sustain it then.

18 MS. LANG: Okay.

19 Q (By Ms. Lang) Your Honor, it's correct, though, that
20 those types of information are what leads you to believe
21 there's probable cause that a crime is committed.

22 MR. FEIN: I'm going to object to that. That's a
23 conclusion. He's already stated what he thought. And ---

24 THE COURT: I'll sustain the objection.

25 MS. LANG: All right.

1 Q (By Ms. Lang) You're a neutral judge in this case,
2 correct?

3 A Correct.

4 Q Undetached from this investigation and this Defendant?

5 A My only involvement, as I recall it, because I don't
6 recognize the name of someone who would have then shown up in
7 front of me later on a criminal docket, my only involvement
8 would have been the execution of this search warrant.

9 Q Did you rubber-stamp the search warrants in any way?

10 MR. FEIN: Object, Your Honor.

11 THE COURT: Overruled.

12 MR. FEIN: All right.

13 A No.

14 Q (By Ms. Lang) You didn't just decide to wholly abandon
15 your judicial role as a neutral judge and just sign it,
16 anyway.

17 A I did not.

18 Q And if a search warrant, you feel like, does not have
19 probable cause, is missing something, there's probably been
20 times you've turned a search warrant away, correct?

21 A Absolutely.

22 Q And have you ever signed search warrants involving drugs,
23 for example, such as heroin?

24 A Yes.

25 Q And do you know the chemical compound or make-up of

1 heroin?

2 A No idea.

3 Q And have you ever signed search warrants dealing with
4 murder victims? A case involving a murder?

5 A Yes.

6 Q And have you -- Do you have a degree in Pathology? Would
7 you be able to tell how someone was murdered by looking at a
8 body?

9 A No.

10 Q If there was a line in the search warrant that said that
11 the method that they were using on this particular day and
12 time for this -- to find this file ---

13 MR. FEIN: Objection; improper hypothetical.

14 THE COURT: Sustained.

15 Q (By Ms. Lang) If there was -- As to this affidavit, --

16 THE COURT: Okay.

17 Q -- if there was information that said this method was 98
18 percent accurate, would that bolster ---

19 MR. FEIN: I object. That's a hypothetical as well.

20 MS. LANG: All right.

21 THE COURT: Yeah. I'm not quite sure where you're
22 going.

23 MS. LANG: I'll leave it at that. Thank you,
24 Your Honor.

25 THE COURT: Okay.

1 MR. FEIN: I just have two questions.

2 THE COURT: Okay. Mr. Fein?

3 REDIRECT EXAMINATION

4 QUESTIONS BY MR. FEIN:

5 Q The Government just asked you about -- or read to you
6 Paragraph 21. If you could just look at that very quickly,
7 Your Honor.

8 A Okay.

9 Q The term "can be evaluated," how was it evaluated?

10 A I don't know.

11 Q Have you had search warrants in murder cases before?

12 A I have.

13 Q In those cases there's a decedent. It's a murder case.

14 A Yes.

15 Q There's a suspect.

16 A Typically.

17 Q What were the -- If you can think of one, what were the
18 circumstances involved in the case?

19 A Well, there was a woman who was missing, a woman from
20 Sunset Hills. She was in the midst of getting a divorce from
21 her husband, and her body was eventually discovered in a very
22 remote area, I believe, of Southwest Missouri. And the reason
23 they were able to find the body was a search warrant was
24 executed. There was apparently in all newer vehicles
25 basically like a black box.

1 Q Correct; yes.

2 A And that black box can be turned off, but apparently what
3 this particular suspect did not know was that when you turn
4 your car off and then turn it back on, it automatically -- you
5 have to then again manually turn off the black box. So the
6 download of the information from the black box revealed the
7 car being in one location and then all of a sudden being at
8 another location many hundred miles away. And, in fact, I
9 think your office may have that case now that I think of it.

10 Q I wouldn't be working on that one. It's possible.

11 A And so because all of a sudden this car showed up a
12 hundred miles away without any indication in the black box how
13 it got there, they went to that location, and they were able
14 to find the body.

15 Q And how did they link it to this particular individual?
16 The suspect.

17 A It was his vehicle.

18 Q Okay. So all those facts, you were capable of
19 understanding and grasping all those facts.

20 A Well, I didn't understand how the black box worked. I
21 didn't understand necessarily any of the technology other than
22 they wanted to search this technology because that technology
23 would be able to locate the place of the vehicle.

24 Q Well, no, no. Forgive me. I'm asking about the fact of
25 the death; that the death occurred. All right?

1 A Well, we didn't ---

2 Q So that's fine. It's fine.

3 A Certainly at the time I executed that warrant we didn't
4 have -- we didn't have a body.

5 Q Very good.

6 A So we didn't know there was a death.

7 Q That's why I was asking about a murder. You had
8 testified earlier about a murder, and I was asking about a
9 murder. This is about something else, but that's fine.

10 A Okay.

11 MR. FEIN: I have no further questions, Your Honor.

12 THE COURT: Okay. Anything more, Ms. Lang?

13 MS. LANG: I just have one question.

14 THE COURT: Okay.

15 RECROSS EXAMINATION

16 QUESTIONS BY MS. LANG:

17 Q Do you know the mechanics working behind the download of
18 the black box in the car?

19 A Absolutely not.

20 MS. LANG: That's it.

21 THE COURT: Okay. Now Mr. Fein.

22 REDIRECT EXAMINATION

23 QUESTIONS BY MR. FEIN:

24 Q All you needed to understand for that case was that the
25 black box is on or off, correct?

1 A Yes.

2 Q You didn't need to understand anything more than it was
3 operating or not operating.

4 A Well, I -- I can tell you that all that information that
5 I sort of relayed earlier was all learned after the fact. At
6 the time they wanted to see what the information was in the
7 black box, not whether it was turned on or off.

8 Q Correct. So all they wanted was, "Your Honor, we need a
9 warrant for the black box in the car," correct?

10 A Not just physically possessing it; to be able to download
11 the ---

12 Q To search it, --

13 A Yes.

14 Q -- right? They came to you for a warrant to search the
15 black box.

16 A Yes.

17 Q All you needed to know was the relationship between the
18 black box and the case, whether or not there was probable
19 cause to search that black box.

20 A Yeah. I'm not sure what you're asking me.

21 Q You signed a warrant to search a black box.

22 A Right. But the basis of it wasn't necessarily that this
23 was -- They were not trying to at this point make the case
24 against somebody. This was an effort to go get the
25 information --

1 Q Right.

2 A -- of somebody they suspected.

3 Q Correct.

4 A And in that case, yeah, I understood that they believed
5 this black box would be able to indicate where this vehicle
6 was at certain times when this particular woman turned up
7 missing.

8 Q Correct. And you said, "Okay, there is -- here's a
9 warrant to search the black box for data."

10 A Yeah. I don't know that it was -- It was a -- It was not
11 your typical short affidavit on a search warrant.

12 Q I'm not making any allegation about ---

13 A Yeah.

14 Q I mean it's not even here. It's not even evidence in
15 this court.

16 A Right.

17 Q I'm just saying it was a warrant to search a black box
18 that might be connected to a murder.

19 A Supported by reasons why that black box was important.

20 Q Right; supported by reasons, right? Reasons you
21 understood, correct?

22 MS. LANG: Objection, Your Honor; outside the scope
23 of ---

24 THE COURT: Yes, we are.

25 MR. FEIN: I have no further questions.

1 THE COURT: Okay.

2 THE WITNESS: I'll learn to shut my mouth.

3 THE COURT: You may step down.

4 THE WITNESS: All right. Thank you, Judge. Am I
5 free to go?

6 THE COURT: You are, unless you'd like to stay.

7 THE WITNESS: Well, I think I'm good.

8 THE COURT: All right.

9 THE WITNESS: Thank you.

10 MR. FEIN: I have no further witnesses, Your Honor.

11 THE COURT: Okay.

12 MR. FEIN: So what I wanted to ask the Court is the
13 following.

14 THE COURT: Yes.

15 MR. FEIN: So this matter for me has been a
16 complicated matter to try to wrap my mind around and
17 information has come to light today that I did not have before
18 that is meaningful to some arguments I'd like to advance to
19 the Court. So I would like to file a post-brief hearing.

20 THE COURT: I would like for you to; believe me.

21 MR. FEIN: Now I've got briefs in another case,
22 motions in another case coming due on May 9th, and I've got
23 motions in a case before you in Mr. Blank's case due on May
24 1st. I've got to travel to Baltimore around May 10th.

25 THE COURT: Are you sure Mr. Blank doesn't want to --

1 I'm just kidding.

2 MR. FEIN: I doubt it, Your Honor. He has some good
3 issues, too, I think. Ask Mr. Livergood. So I'm thinking
4 maybe ---

5 THE COURT: Well, first of all, we'll want to get a
6 transcript, correct?

7 MR. FEIN: Right.

8 THE COURT: So we'd like to give our court reporter
9 time --

10 MR. FEIN: She'll need a year, I think.

11 THE COURT: -- to figure out what she just took down
12 in all of that testimony.

13 And do you have an idea of how long a transcript
14 would take?

15 COURT REPORTER: How about two weeks?

16 THE COURT: Two weeks for the transcript. And then
17 once we get the transcript, so ---

18 MR. FEIN: Yeah. Can we maybe look at dates once we
19 get the transcript, Your Honor?

20 THE COURT: Let's see. Where are we now? Today is
21 the 19th. So two weeks would be -- May 3rd would be the
22 transcript will be received.

23 How much time do you think you would need after
24 receipt of the transcript?

25 MR. FEIN: It's going to take me a fair amount of

1 time to write that. There's a number of issues I have to
2 address.

3 THE COURT: Do you think that it would take you a
4 month?

5 MR. FEIN: It could with everything else going on,
6 yes. There are portions of it I can start on with some of
7 the -- without the transcript, but I do have all those other
8 matters.

9 THE COURT: So -- Yeah. I mean I can -- If we go
10 out -- You know, four weeks takes us to -- past the transcript
11 takes us to May 31st.

12 MR. FEIN: Okay. We can use that as -- Can we use
13 that as our date for the moment, anyway?

14 THE COURT: Yes. And if you need additional time,
15 you'll have to file a motion for additional time.

16 And then how much time do you think the Government
17 will need once it receives the response?

18 MS. LANG: Your Honor, at this time I'm going to ask
19 for two weeks.

20 THE COURT: Okay. So at this time what I'm going to
21 do is set a -- the briefing schedule for the Defendant to file
22 supplemental briefing by May 31st, and then the Government to
23 file a response by June 14th. And you're going to want to
24 reply.

25 MR. FEIN: Very likely.

1 THE COURT: You probably will.

2 MR. FEIN: It's likely.

3 THE COURT: I know you. How about a week for the
4 reply?

5 MR. FEIN: That sounds reasonable right now.

6 THE COURT: Okay.

7 MR. FEIN: I'm sure it won't when the time comes.

8 THE COURT: The 21st for the reply?

9 MS. LANG: No objection.

10 THE COURT: Okay.

11 MR. FEIN: Thank you, Your Honor.

12 THE COURT: All right. Thank you very much. That
13 concludes today's hearing, and we are in recess and we are
14 adjourned.

15 (Court adjourned at 3:35 PM.)

16

17

18

19

20

21

22

23

24

25

CERTIFICATE OF OFFICIAL REPORTER

I, Deborah A. Kriegshauser, Federal Official Realtime Court Reporter, in and for the United States District Court for the Eastern District of Missouri, do hereby certify that pursuant to Section 753, Title 28, United States Code, that the foregoing is a true and correct transcript of the stenographically-reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Dated this 24th of April, 2017.

/s/ Deborah A. Kriegshauser

DEBORAH A. KRIEGSHAUSER, FAPR, RMR, CRR
FEDERAL OFFICIAL COURT REPORTER